developer WORLD

Developers guidelines

June 2010

OMA Client Provisioning and Device Management

for Sony Ericsson phones with DM client v.5 – v.6

Sony Ericsson

Preface

Purpose of this document

This document describes the implementation of OMA Client Provisioning and Device Management functionalities in Sony Ericsson phones with Device Management Client version 5.0 or higher. Corresponding Developers guidelines for earlier DM client versions can be found on Developer World.

People who can benefit from this document are:

- Software developers
- Operators and service providers
- Content providers

It is assumed that the reader has a basic understanding of the OMA Client Provisioning and Device Management technologies and standards.

These Developers guidelines are published by:

Sony Ericsson Mobile Communications AB,
SE-221 88 Lund, Sweden

www.sonyericsson.com/

14th edition (June 2010)
Publication number: 1214-8437.14

Sony Ericsson Developer World

At www.sonyericsson.com/developer, developers find the latest technical documentation and development tools such as phone White papers, Developers guidelines for different technologies, Getting started tutorials, SDKs (Software Development Kits) and tool plugins. The Web site also features news articles, go-to-market advice, moderated discussion forums offering free technical support and a Wiki community sharing expertise and code examples.

For more information about these professional services, go to the Sony Ericsson Developer World Web site.

Trademarks and acknowledgements

Document conventions

Products

Sony Ericsson phones are referred to in this document by generic names as follows:

Generic names	Sony Ericsson phones	Device Management	
Series		client version	protocol version
Aino™	Aino™ U10i, Aino™ U10a	6.0	1.2
C510	C510, C510c, C510a	5.0	1.2
C901	C901, C901a, C901 GreenHeart™	5.0	1.2
C903	C903, C903a	5.0	1.2
C905	C905, C905c, C905a	5.0	1.2
Cedar	Sony Ericsson Cedar™ J108i, Sony Ericsson Cedar™ J108a	6.0	1.2
Elm	Sony Ericsson Elm™ J10, Sony Ericsson Elm™ J10i2	6.0	1.2
G705	G705, G705u	5.0	1.2
Hazel	Sony Ericsson Hazel™ J20, Sony Ericsson Hazel™ J20i	6.0	1.2
Jalou™	Jalou™ F100i, BeJoo™ F100i	5.0	1.2
Naite™	Naite™ J105i, Naite™ J105a	5.0	1.2
Pureness™	Xperia™ Pureness™ X5, Xperia™ Pureness™ X5i	6.0	1.2
T707	T707, T707a	5.0	1.2
T715	T715, T715a	5.0	1.2
W508	W508, W508c, W508a, W518a	5.0	1.2
W705	W705, W705u	5.0	1.2
W715	W715	5.0	1.2
W995	W995, W995a	5.0	1.2
X5	Xperia™ Pureness™ X5, X5i	6.0	1.2
Yari™	Yari™ U100i, Yari™ U100a	6.0	1.2
Zylo	Sony Ericsson Zylo™ W20, Sony Ericsson Zylo™ W20i	6.0	1.2

Terminology and abbreviations

APN	Access Point Name
CP	Client Provisioning. This is the process by which a WAP client is initially configured with connectivity and application access parameters. This is a non-interactive process as opposed to Device Management
CSD	Circuit Switched Data
DDF	Device Description Framework. This framework prescribes a way for device vendors to describe their devices so that a management system can understand how to manage the device
DM	Device Management. A set of OMA (Open Mobile Alliance) standard mechanisms that enables remote interactive configuration of, for example, a phone
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
IMPS	Instant Messaging and Presence Service according to OMA standards
IMS	IP Multimedia Subsystem
MAC	Message Authentication Code
MCC	Mobile Country Code
MO	Management Object. Management objects are the entities that can be manipulated by management actions carried over the SyncML DM protocol
OMA	Open Mobile Alliance. The primary standardisation organisation for mobile applications. See http://www.openmobilealliance.org
OTA	Over-The-Air
PSD	Packet Switched Data
SIM	Subscriber Identity Module. In the rest of the document the term SIM is used to denote the traditional GSM SIM as well as the USIM and UICC
SMS	Short Message Service
SMS-C	Short Message Service Centre
TLS	Transport Layer Security
TPS	Trusted Provisioning Server
UICC	USIM Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identity Module
WAP	Wireless Application Protocol
WBXML	WAP Binary Extended Markup Language
WIM	Wireless Identification Module

WLAN	Wireless Local Area Network
XML	Extended Markup Language

Typographical conventions

Code is written in Courier font: `<characteristic>...</characteristic>`

String values are written inside double quotation marks: “`Off`”

Document history

Change history		
2008-06-18	Doc no. 1214-8437.1	First version published on Developer World. Information about C905
2008-07-22	Doc no. 1214-8437.2	Second version. Minor revision
2008-09-09	Doc no. 1214-8437.3	Third version. Information about G705 added
2008-10-17	Doc no. 1214-8437.3 (rev. B)	Third revised version. New document layout.
2008-11-11	Doc no. 1214-8437.4	Fourth version. Information about W705 added
2009-01-08	Doc no. 1214-8437.5	Fifth version. Information about C510 and W508 series added
2009-02-15	Doc no. 1214-8437.6	Sixth version. Information about C901, C903, W715 and W995 series added
2009-03-26	Doc no. 1214-8437.7	Seventh version. Information about T707 series added
2009-05-28	Doc no. 1214-8437.8	Eighth version. Information about DM client v.6 and Aino™ and Yari™ phone series added
2009-06-25	Doc no. 1214-8437.9	Ninth version. Information about Naite™ and T715 phone series added
2009-08-12	Doc no. 1214-8437.10	Tenth version. Information about Jalou™ phone series added
2009-10-26	Doc no. 1214-8437.11	11th version. Information about Pureness™ phone series added
2009-12-14	Doc no. 1214-8437.12	12th version. Information about Elm and Hazel phone series added
2010-04-13	Doc no. 1214-8437.13	13th version. Information about Zylo phone series added
2010-06-17	Doc no. 1214-8437.14	14th version. Information about Cedar phone series added

Contents

OMA Client Provisioning

OMA Client Provisioning v1.1 (WAP OMA Provisioning), is a backward-compatible extension of the client provisioning functionality included in WAP 2.0 (v1.0). The new version adds support for application access provisioning as well as direct access and WAP proxy support.

Introduction

With OMA Client Provisioning v1.1 it is possible, for example, for an operator or service provider to configure (bootstrap) the terminal with settings for different applications in phones (browser, email, streaming, OMA Data Synchronisation, Device Management, Wireless Village and so on). The bootstrap process is initiated when an unconfigured phone is started from its initial state or after a master reset.

The bootstrap process normally includes configuration parameters for WAP services including the identification parameters for the Trusted Provisioning Server (TPS). This server includes a Provisioning Manager, that controls continuous provisioning.

The Sony Ericsson implementation supports bootstrap from SIM and over-the-air (OTA) via SMS.

Sony Ericsson Symbian OS™ phones (smartphones) also implement interfaces for client provisioning through provisioning documents in the internal file system or on a memory card, transferred via Infrared or Bluetooth™, delivered as email attachments, or downloaded from Web pages.

The basis of client provisioning is the Provisioning Document (ProvDoc). This is an XML or WBXML encoded message containing a list of characteristics specifying the settings to be provisioned. A ProvDoc can be pushed to a phone using a WAP push message. This is normally done by an operator or service provider to configure a phone owned by one of their users.

The OMA Client Provisioning specification allows ProvDocs to be stored on a SIM or UICC card. When the phone starts, the client provisioning framework checks if the smartcard inserted is the same one that was inserted the last time the phone was started. If not, or if this is the first time the phone is started, the framework will look for ProvDocs on the smartcard. If new ProvDocs are detected, they are submitted for processing.

For details on the OMA Client Provisioning v1.1 standard, see the documentation found at
http://www.openmobilealliance.org/.

Supported standards

The provisioning documents are delivered as WAP binary XML documents (WBXML) using the UTF-8 [RFC2279] character encoding set. These documents are delivered over-the-air using a bootstrap protocol, see Provisioning Bootstrap 1.1, Open Mobile Alliance, OMA-WAP-PROVBOOT-V1_1,
http://www.openmobilealliance.org/.

The details of the bootstrap protocol, particularly the security mechanism, depend on the technology used, but the basic mechanism which uses connectionless WAP Push refers to WAP Push OTA Specification WAP Forum, WAP-235-PushOTA,
http://www.openmobilealliance.org/. The specification also defines mandatory security mechanisms that can be used with all network technologies.

As an option, the provisioning documents can be delivered via WIM or SIM cards. The Requester interface design for SIM/WIM provisioning is described in Provisioning Smart Card 1.1, Open Mobile Alliance, OMA-WAP-PROVSC-V1_1, http://www.openmobilealliance.org/. There are three different storage areas supported by Sony Ericsson client provisioning on the card: Bootstrap, Config1 and Config2.

The standards provide rules for how the security mechanisms are to be used and how the provisioning documents delivered through different channels must be combined. There are also rules for how to implement conflict resolution, error handling, proxy selection and parameter prioritisation when interpreting the provisioning documents received. These aspects are covered in Provisioning User Agent Behaviour 1.1, Open Mobile Alliance, OMA-WAP-PROVUABV1_1, http://www.openmobilealliance.org/.

Document reception

Provisioning documents can be made available to the phone via several different methods and media.

Note: The documents are processed only when the phone is in standby mode, in all other cases the documents are queued. If the phone is not in standby mode, the user does not notice the reception of a provisioning document. The next time the phone is in standby mode, the user is prompted to install the settings.

OTA

One or several SMS messages (maximum supported number is 20) are sent with destination port 2948 (non-secure WAP Push). These SMS messages are reassembled, parsed and handled by the provisioning user agent in the phone. The user is prompted whether to install the provisioning settings received or not. If the user accepts, the phone is configured with the new settings.

Depending on whether the settings were successfully stored in the phone or not, the user receives a report message stating which application the settings were successfully installed for, or if they were not installed.

If the user does not accept the new settings, they are rejected and are not stored in the phone.

See WAP Push OTA Specification" WAP Forum, WAP-235-PushOTA, http://www.openmobilealliance.org. This specification also defines mandatory security mechanisms that can be used with all network technologies.

SIM

Provisioning documents can be delivered via WIM or SIM cards.

This method is usually used for the initial provisioning of new phones and reprovisioning after a master reset. In these situations, provisioning needs to be done to set all basic parameter values correctly.

When the phone starts, differences between configuration settings are compared to those residing on the WIM/SIM. Three different storage areas, Bootstrap, Config1 and Config2 on the smartcard, may contain provisioning documents. If the provisioning handling framework detects that provisioning needs to be done, the document on the smartcard is parsed and the read parameter settings are stored in the provisioning parameter tree.

The Requester interface design for SIM/WIM provisioning is described in Provisioning Smart Card 1.1, Open Mobile Alliance, OMA-WAP-PROVSC-V1_1, http://www.openmobilealliance.org/.

Security mechanisms

To prevent non-authorised people from sending malicious content to users, four different alternative security features have been implemented: UserPin, UserPinMac, NetwPin and UserNetwPin. See Provisioning Bootstrap 1.1, Open Mobile Alliance, OMA-WAP-PROVBOOT-V1_1, http://www.openmobilealliance.org/.

The security features NetwPin and UserNetwPin are bound to the IMSI of the SIM card, so they only work for the SIM they are created for.

In cases where the security mechanism requires the user to enter a PIN, the user is allowed three attempts to enter the numbers correctly, otherwise the document is rejected.

Parameters and compliance

NAPDEF

NAPDEF is mapped to the Sony Ericsson data account, allowing the phone to connect to the Internet, send MMS and email and so on. The data account is used to gather connectivity settings such as what bearer to use, APN, authentication information and QoS. To each data account it is possible to set three proxies, one for HTTP connections, one for secure connections and one for streaming. The proxies are created using characteristics PXLOGICAL and PXPHYSICAL and are linked to the data account using PXLOGICAL/PXPHYSICAL/TO-NAPID.

There can be maximum 25 data accounts installed. A data account is never overwritten, instead a new one is created. If a data account is provisioned with the same name as an already installed account, the new one gets a suffix containing a dash and a number, for example, “account-2”.

The table lists supported parameters in reference to *OMA-WAP-ProvCont-v1_1-20050428-C.pdf, chapter 4.2 Overview of Data Model*.

In the Usage column, the following abbreviations are used:
I = Ignored, M = Mandatory, N = Not used, and O = Optional.

Parameter	Usage	Description
Characteristic : NAPDEF	O	Mapped to Sony Ericsson data account
NAPID	M	Reference identity of the NAPDEF characteristics
BEARER	M	GSM-CSD, GSM-GPRS, WLAN. For 3G enabled phones GSM-CSD is mapped to 3G CS and GSM-GPRS is mapped to 3G PS. WLAN is mapped to local bearer
NAME	M	Sets the name for the corresponding data account
INTERNET	N	
NAP-ADDRESS	M/O	Mandatory if BEARER = GSM-GPRS or GSM-CSD. Specifies APN for GSM-GPRS, CSD dial string for GSM-CSD. Optional if BEARER = WLAN
NAP-ADDRTYPE	I	Only support for IPV4 (GSM-GPRS) and E164 (GSM-CSD), which are therefore the assumed values
DNS-ADDR	O	DNS
CALLTYPE	O	CSD dial type. ANALOG-MODEM, V.120 or V.110
LOCAL-ADDR	O	GPRS IP or WLAN host address
LOCAL-ADDRTYPE	I	Only IPv4 supported, and is therefore the assumed value
LINKSPEED	N	
DNLINKSPEED	O	CSD downlink data rate
LINGER	O	Inactivity timeout
DELIVERY-ERR-SDU	N	
DELIVERY-ORDER	N	
TRAFFIC-CLASS	O	See 3GPP TS 23.107 and 3GPP TS 24.008
MAX-SDU-SIZE	N	
MAX-BITRATE-UPLINK	N	
MAX-BITRATE-DNLINK	O	See 3GPP TS 23.107 and 3GPP TS 24.008
RESIDUAL-BER	O	See 3GPP TS 23.107 and 3GPP TS 24.008
SDU-ERROR-RATIO	O	See 3GPP TS 23.107 and 3GPP TS 24.008

In the Usage column, the following abbreviations are used: *I = Ignored, M = Mandatory, N = Not used, and O = Optional.*		
Parameter	**Usage**	**Description**
TRAFFIC-HANDL-PRIO	O	See 3GPP TS 23.107 and 3GPP TS 24.008
TRANSFER-DELAY	N	
GUARANTEED-BITRATE-UPLINK	N	
GUARANTEED-BITRATE-DNLINK	N	
MAX-NUM-RETRY	N	
FIRST-RETRY-TIMEOUT	N	
REREG-THRESHOLD	N	
T-BIT	N	
NAPDEF : NAPAUTHINFO	O	
AUTHTYPE	O	Supported values are PAP or CHAP
AUTHNAME	O	Data account username
AUTHSECRET	O	Data account password
AUTH-ENTITY	N	
SPI	N	
NAPDEF : VALIDITY	N	
COUNTRY	N	
NETWORK	N	
SID	N	
SOC	N	
VALIDUNTIL	N	
NAPDEF:WLAN	O	Mandatory if BEARER = WLAN
PRI-SSID	M	Name of the WLAN network
NET_MODE	O	INFRA or ADHOC. Default: INFRA
SEC-MODE	O	WEP, WPA-PRESHARED-KEY or WPA2-PRESHARED-KEY. If omitted, no security is applied
WPA-PRES-KEY-ASC	O	Pre-shared key for WPA encryption, 8 – 63 ASCII characters. Has precedence over WPA-PRES-KEY-HEX if both are present. Only used if SEC-MODE is WPA-PRESHARED-KEY or WPA2-PRESHARED-KEY

In the Usage column, the following abbreviations are used: *I = Ignored, M = Mandatory, N = Not used, and O = Optional.*		
Parameter	**Usage**	**Description**
WPA-PRES-KEY-HEX	O	Pre-shared key for WPA encryption, 32-bit hex value. Base64 encoded. Only used if SEC-MODE is WPA-PRESHARED-KEY or WPA2-PRESHARED-KEY
WEPKEYIND	O	Indicates index of the key to be used within WLAN : WEPKEY. Possible values: 0 – 3. Only used if SECMODE = WEP
WEPAUTHMODE	O	OPEN or SHARED. Only valid if SEC-MODE = WEP
WLAN : WEPKEY	O	May only occur within WLAN. Maximum four WEPKEY characteristics can be present within WLAN.
LENGTH	O	Length of the WEP key in number of bits
INDEX	O	Index of the WEP key
DATA	O	The WEP key encoded as Base64

The following provisioning example illustrates a NAPDEF account for WLAN with no security:

```
<wap-provisioningdoc version="1.1">
     <characteristic type="NAPDEF">
          <parm name="NAPID" value="NAP1"/>
          <parm name="BEARER" value="WLAN"/>
          <parm name="NAME" value="MY WLAN"/>
          <characteristic type="WLAN">
               <parm name="PRI-SSID" value="MYWLAN"/>
               <parm name="NETMODE" value="INFRA"/>
          </characteristic>
     </characteristic>
</wap-provisioningdoc>
```

The following example illustrates a NAPDEF account for WLAN with four shared WEP keys:

```
<wap-provisioningdoc version="1.1">
     <characteristic type="NAPDEF">
          <parm name="NAPID" value="NAP1"/>
          <parm name="BEARER" value="WLAN"/>
          <parm name="NAME" value="MY WLAN 2"/>
          <characteristic type="WLAN">
               <parm name="PRI-SSID" value="MYWLAN2"/>
               <parm name="NETMODE" value="INFRA"/>
               <parm name="SECMODE" value="WEP"/>
               <parm name="WEPAUTHMODE" value="SHARED"/>
               <parm name="WEPKEYIND" value="2"/>
               <characteristic type="WEPKEY">
                    <parm name="LENGTH" value="64"/>
                    <parm name="INDEX" value="0"/>
                    <parm name="DATA" value="YWJjZGU="/>
               </characteristic>
```

```
                <characteristic type="WEPKEY">
                     <parm name="LENGTH" value="64"/>
                     <parm name="INDEX" value="1"/>
                     <parm name="DATA" value="ZmdoaWo="/>
                </characteristic>
                <characteristic type="WEPKEY">
                     <parm name="LENGTH" value="64"/>
                     <parm name="INDEX" value="2"/>
                     <parm name="DATA" value="a2xtbm8="/>
                </characteristic>
                <characteristic type="WEPKEY">
                     <parm name="LENGTH" value="64"/>
                     <parm name="INDEX" value="3"/>
                     <parm name="DATA" value="cHFyc3Q="/>
                </characteristic>
          </characteristic>
     </characteristic>
</wap-provisioningdoc>
```

The following example illustrates a NAPDEF account for WLAN with a preshared WPA key:

```
<wap-provisioningdoc version="1.1">
     <characteristic type="NAPDEF">
          <parm name="NAPID" value="NAP1"/>
          <parm name="BEARER" value="WLAN"/>
          <parm name="NAME" value="MY WLAN 3"/>
          <characteristic type="WLAN">
               <parm name="PRI-SSID" value="MYWLAN3"/>
               <parm name="NETMODE" value="INFRA"/>
               <parm name="SECMODE" value="WPA-PRESHARED-KEY"/>
               <parm name="WPA-PRES-KEY-ASC" value="My first
passphrase"/>
          </characteristic>
     </characteristic>
</wap-provisioningdoc>
```

The following example illustrates a NAPDEF account for CSD :

```
<wap-provisioningdoc version="1.1">
     <characteristic type="NAPDEF">
          <parm name="NAPID" value="NAP-CSD"/>
          <parm name="BEARER" value="GSM-CSD"/>
          <parm name="NAME" value="CSD Account"/>
          <parm name="NAP-ADDRESS" value="+46012345678"/>
          <parm name="DNS-ADDR" value="10.11.12.13"/>
          <parm name="CALLTYPE" value="ANALOG-MODEM"/>
          <parm name="DNLINKSPEED" value="9600"/>
     </characteristic>
</wap-provisioningdoc>
```

The following example illustrates a NAPDEF account for GSM/GPRS :

```
<wap-provisioningdoc version="1.1">
     <characteristic type="NAPDEF">
```

```
            <parm name="NAPID" value="NAP1" />
            <parm name="BEARER" value="GSM-GPRS" />
            <parm name="NAME" value="Operator dataacc name" />
            <parm name="NAP-ADDRESS" value="online.operator.se" />
            <parm name="NAP-ADDRTYPE" value="IPV4" />
            <characteristic type="NAPAUTHINFO">
                 <parm name="AUTHTYPE" value="PAP" />
                 <parm name="AUTHNAME" value="Username" />
                 <parm name="AUTHSECRET" value="Password" />
            </characteristic>
       </characteristic>
</wap-provisioningdoc>
```

PXLOGICAL

PXLOGICAL is used to define proxies that should be used by a data account. It is possible to define up to three proxies of different types per data account. This is done either by including up to three PXLOGICAL (each with one PXPHYSICAL), or one PXLOGICAL with up to three PXPHYSICAL. The type of the proxy is determined by the parameter PORT/SERVICE.

PORT/SERVICE	Resulting proxy type
OTA-HTTP-TO	HTTP proxy
OTA-HTTP-PO	HTTP proxy
OTA-HTTP-TLS-TO	Secure proxy
OTA-HTTP-TLS-PO	Secure proxy
CL-WSP	Invalid service
CO-WSP	Invalid service
CL-SEC-WSP	Invalid service
CO-SEC-WSP	Invalid service
CL-SEC-WTA	Invalid service
CO-SEC-WTA	Invalid service

If PORT/SERVICE is missing, PORT/PORTNBR is used to determine the proxy type.

PORT/PORTNBR	Resulting proxy type
554	Streaming proxy
443	Secure proxy
All other valid port numbers	HTTP proxy
9200-9207	Invalid ports

The table below lists supported parameters in reference to *OMA-P-ProvCont-v1_1-20050428-C.pdf, chapter 4.2 Overview of Data Model*.

In the Usage column, the following abbreviations are used: *I = Ignored, M = Mandatory, N = Not used, and O = Optional.*		
Parameter	**Usage**	**Description**
Characteristic : PXLOGICAL	O	Mapped to Proxy settings in data account
PROXY-ID	M	Reference identity of the PXLOGICAL characteristic
PROXY-PW	N	
PPGAUTH-TYPE	N	
PROXY-PROVIDER-ID	N	
NAME	M	
DOMAIN	N	
TRUST	N	
MASTER	N	
STARTPAGE	O	Sets the URL for the homepage. See also APPID "w2"
BASAUTH-ID	N	
BASAUTH-PW	N	
WSP-VERSION	N	
PUSHENABLED	N	
PULLENABLED	N	
PXLOGICAL : PXAUTHINFO	O	
PXAUTH-TYPE	I	HTTP-BASIC is the only supported value and is therefore the assumed value
PXAUTH-ID	O	Proxy username
PXAUTH-PW	O	Proxy password
PXLOGICAL : PORT	O	PORT can either be used in PXLOGICAL or PXPHYSICAL
PORTNBR	M	For supported ports, see table on page 18
SERVICE	O	For supported services, see table on page 18
PXLOGICAL : PXPHYSICAL	M	1, 2 or 3 PXPHYSICAL supported per PXLOGICAL
PHYSICAL-PROXY-ID	M	An application can use this parameter
DOMAIN	N	
PXADDR	M	Proxy address

In the Usage column, the following abbreviations are used: *I = Ignored, M = Mandatory, N = Not used, and O = Optional.*		
Parameter	**Usage**	**Description**
PXADDRTYPE	I	Only IPV4 is supported and is therefore the assumed value
PXADDR-FQDN	O	Proxy address as FQDN
WSP-VERSION	N	
PUSHENABLED	N	
PULLENABLED	N	
TO-NAPID	M	Links the proxy settings to a data account
PXPHYSICAL : PORT	O	PORT can either be used in PXLOGICAL or PXPHYSICAL
PORTNBR	M	For supported ports, see table on page 18
SERVICE	O	For supported services, see table on page 18

The following example uses three PXPHYSICAL within the same PXLOGICAL to create a data account with one HTTP, one secure and one streaming proxy associated with it. The authentication data (PXAUTHINFO) is applied to all three proxies. Please note that the same value of TO-NAPID must be used in all three PXPHYSICAL.

```
<wap-provisioningdoc version="1.1">
     <characteristic type="PXLOGICAL">
          <parm name="PROXY-ID" value="Proxy1"/>
          <parm name="NAME" value="Not used"/>
          <parm name="STARTPAGE"
value="http://www.sonyericsson.com"/>

          <characteristic type="PXAUTHINFO">
               <parm name="PXAUTH-TYPE" value="HTTP-BASIC"/>
               <parm name="PXAUTH-ID" value="username"/>
               <parm name="PXAUTH-PW" value="password"/>
          </characteristic>

          <characteristic type="PXPHYSICAL">
               <parm name="PHYSICAL-PROXY-ID" value="HttpProxy"/>
               <parm name="PXADDR" value="111.111.111.111"/>
               <parm name="PXADDRTYPE" value="IPV4"/>
               <parm name="TO-NAPID" value="NAP1"/>
          </characteristic>

          <characteristic type="PXPHYSICAL">
               <parm name="PHYSICAL-PROXY-ID"
value="SecureProxy"/>
               <parm name="PXADDR" value="111.111.111.112"/>
               <parm name="PXADDRTYPE" value="IPV4"/>
               <parm name="TO-NAPID" value="NAP1"/>
               <characteristic type="PORT">
                    <parm name="SERVICE" value="OTA-HTTP-TLS-TO"/
>
```

```
                    <parm name="PORTNBR" value="1234"/>
               </characteristic>
          </characteristic>

          <characteristic type="PXPHYSICAL">
               <parm name="PHYSICAL-PROXY-ID"
value="StreamingProxy"/>
               <parm name="PXADDR" value="111.111.111.113"/>
               <parm name="PXADDRTYPE" value="IPV4"/>
               <parm name="TO-NAPID" value="NAP1"/>
               <characteristic type="PORT">
                    <parm name="PORTNBR" value="554"/>
               </characteristic>
          </characteristic>
     </characteristic>

     <characteristic type="NAPDEF">
          <parm name="NAPID" value="NAP1"/>
          <parm name="BEARER" value="GSM-GPRS"/>
          <parm name="NAME" value="Data Account Name"/>
          <parm name="NAP-ADDRESS" value="222.222.222.222"/>
          <parm name="NAP-ADDRTYPE" value="IPv4"/>
     </characteristic>
</wap-provisioningdoc>
```

Alternatively the following example with three PXLOGICAL could be used. Using this method it is possible to set different authentication data on the three proxies.

```
<characteristic type="PXLOGICAL">
     <parm name="PROXY-ID" value="Proxy1"/>
     <parm name="NAME" value="Not used"/>
     <parm name="STARTPAGE"
value="http://www.sonyericsson.com"/>
     <characteristic type="PXAUTHINFO">
          <parm name="PXAUTH-TYPE" value="HTTP-BASIC"/>
          <parm name="PXAUTH-ID" value="username1"/>
          <parm name="PXAUTH-PW" value="password1"/>
     </characteristic>
     <characteristic type="PXPHYSICAL">
          <parm name="PHYSICAL-PROXY-ID" value="HttpProxy"/>
          <parm name="PXADDR" value="111.111.111.111"/>
          <parm name="PXADDRTYPE" value="IPV4"/>
          <parm name="TO-NAPID" value="NAP1"/>
     </characteristic>
</characteristic>

<characteristic type="PXLOGICAL">
     <parm name="PROXY-ID" value="Proxy2"/>
     <parm name="NAME" value="Not used"/>
     <characteristic type="PXAUTHINFO">
          <parm name="PXAUTH-TYPE" value="HTTP-BASIC"/>
          <parm name="PXAUTH-ID" value="username2"/>
          <parm name="PXAUTH-PW" value="password2"/>
     </characteristic>
     <characteristic type="PXPHYSICAL">
```

```
          <parm name="PHYSICAL-PROXY-ID" value="SecureProxy"/>
          <parm name="PXADDR" value="111.111.111.112"/>
          <parm name="PXADDRTYPE" value="IPV4"/>
          <parm name="TO-NAPID" value="NAP1"/>
          <characteristic type="PORT">
               <parm name="SERVICE" value="OTA-HTTP-TLS-TO"/>
               <parm name="PORTNBR" value="1234"/>
          </characteristic>
     </characteristic>
</characteristic>

<characteristic type="PXLOGICAL">
     <parm name="PROXY-ID" value="Proxy3"/>
     <parm name="NAME" value="Not used"/>
     <characteristic type="PXAUTHINFO">
          <parm name="PXAUTH-TYPE" value="HTTP-BASIC"/>
          <parm name="PXAUTH-ID" value="username3"/>
          <parm name="PXAUTH-PW" value="password3"/>
     </characteristic>
     <characteristic type="PXPHYSICAL">
          <parm name="PHYSICAL-PROXY-ID" value="StreamingProxy"/>
          <parm name="PXADDR" value="111.111.111.113"/>
          <parm name="PXADDRTYPE" value="IPV4"/>
          <parm name="TO-NAPID" value="NAP1"/>
          <characteristic type="PORT">
               <parm name="PORTNBR" value="554"/>
          </characteristic>
     </characteristic>
</characteristic>

<characteristic type="NAPDEF">
     <parm name="NAPID" value="NAP1"/>
     <parm name="BEARER" value="GSM-GPRS"/>
     <parm name="NAME" value="Data Account Name"/>
     <parm name="NAP-ADDRESS" value="222.222.222.222"/>
     <parm name="NAP-ADDRTYPE" value="IPv4"/>
</characteristic>
```

BOOTSTRAP

The bootstrap process is performed the first time a SIM is inserted in the phone. A restart of the bootstrap process is also done after a master reset. After the phone is bootstrapped, an incoming provisioning document should be handled according to the table. Note that no overwrite is done without user permission.

In the Usage column, the following abbreviations are used:
I = Ignored, M = Mandatory, N = Not used, and O = Optional.

Parameter	Usage	Description
Characteristic : BOOTSTRAP	O	
NAME	O	Used as title when presenting the document to the user
NETWORK	N	
COUNTRY	N	
PROXY-ID	N	
PROVURL	O	The identifier of the context
CONTEXT-ALLOW	O	Specifies how many more contexts can be installed

Bootstrap example:

```
     <characteristic type="BOOTSTRAP">
          <parm name="NAME" value="Operator settings name"/>
          <parm name="CONTEXT-ALLOW" value="255"/>
          <parm name="PROVURL"
value="http://www.sonyericsson.com"/>
     </characteristic>
```

CLIENTIDENTITY

Clientidentity may be used to define a global identity.

In the Usage column, the following abbreviations are used:
I = Ignored, M = Mandatory, N = Not used, and O = Optional.

Parameter	Usage	Description
Characteristic : CLIENTIDENTITY	O	
CLIENT-ID	O	Fallback value of PXAUTH-ID

Application specific settings

Note: All applications might not be configurable for a specific phone.

The value of the parameter APPID in the APPLICATION element identifies which application settings are to be applied. For more information about the different tags, see the standards for the respective application.

The following application references are supported:

APPID	Application
w2	Browser
w4	MMS
w5	OMA Data Synchronisation
w7	OMA Device Management
25	Email, SMTP
110	Email, POP3
143	Email, IMAP4
554	Streaming media
wA	IMPS (WV) (Not in phones with DM version 6)
ap0004	Positioning
ap2001	IMS (IP Multimedia Subsystem). (Not in phones with DM version 6)
x-semc-mobile-tv	Sony Ericsson MobileTV Not supported in all phones
x-semc-gan-service	Sony Ericsson Generic Access Network (GAN) service

Application references:

Parameter	Usage	Description
Characteristic : APPLICATION	Optional	All tags in the characteristic APPLICATION are supported. For the behaviour of each application, see the specification for each APPID

Browser - APPID “w2”

OMA Application Characteristic reference

APPID: w2

APPID type: OMNA

Owner: OMA DM Working Group

Contact: OMA DM Working Group <OMA-DM@MAIL.OPENMOBILEALLIANCE.ORG>

Registration version: 1

Registration timestamp: 2003-01-24

Application description: Browser

Description - “w2”

Settings for the browser application.

New provisioned settings overwrite the old ones, but do not reset them.

It is possible to set the following via the browser:

- Data account (NAPDEF) to be used as default
- Start page for the data account
- Bookmarks.

Compliance

In the Usage column, the following abbreviations are used:
I = Ignored, M = Mandatory, N = Not used, and O = Optional.

Parameter	Usage	Description
Characteristic : APPLICATION		
APPID	M	“w2”
TO-NAPID	O	Refers to the NAPDEF (data account) to be set as default
APPLICATION : RESOURCE	O	
URI	M	URL
NAME	O	Title of the bookmark or start page. Max size 16
STARTPAGE	O	The first RESOURCE with STARTPAGE is set as STARTPAGE for the data account referenced by TO-NAPID

Example

This example installs two bookmarks and sets the start page for the PXLOGICAL to www.operator.com.

```
<characteristic type="APPLICATION">
     <parm name="APPID" value="w2"/>
     <parm name="TO-NAPID" value="NAP1" />
     <characteristic type="RESOURCE">
          <parm name="URI" value="www.operator.com/"/>
          <parm name="NAME" value="Some Operator WAP Service"/>
          <parm name="STARTPAGE"/>
     </characteristic>
     <characteristic type="RESOURCE">
          <parm name="URI" value="www.somewhere.com/ "/>
          <parm name="NAME" value="Bookmark 1"/>
     </characteristic>
     <characteristic type="RESOURCE">
          <parm name="URI" value="www.nowhere.com/ "/>
          <parm name="NAME" value="Bookmark 2"/>
     </characteristic>
</characteristic>
```

MMS - APPID “w4”

OMA Application Characteristic reference

APPID: w4

APPID type: OMNA

Owner: OMA Multimedia Messaging Working Group

Contact: OMA Multimedia Messaging Working Group <OMA-MMS@MAIL.OPENMOBILEALLIANCE.ORG>

Registration version: 1

Registration timestamp: 2003-01-20

Application description: Multimedia Messaging Service (MMS)

Application reference: Multimedia Messaging Service (MMS) specifications, http://www.wapforum.org/what/technical.htm

Description - “w4”

Sets the service centre and data account to be used for connection.

The settings for this application are grouped into accounts and maximum 10 accounts can be installed. An installed account is not overwritten, instead a new account is created.

Compliance

In the Usage column, the following abbreviations are used:
I = Ignored, M = Mandatory, N = Not used, and O = Optional.

Parameter	Usage	Description
Characteristic : APPLICATION		
APPID	M	“w4”
NAME	O	Name of account. If missing, data account name is used
TO-NAPID	M	Reference to NAPDEF (data account)
ADDR	(M)	Service centre. Mandatory if APPLICATION:APPADDR:ADDR not set
APPLICATION : APPADDR	O	
ADDR	(M)	Secondary method for setting service centre. Mandatory if APPLICATION:ADDR not set

Example

This example sets the service centre and data account to use for connection.

```
<characteristic type="APPLICATION">
     <parm name="APPID" value="w4"/>
     <parm name="TO-NAPID" value="MMS-NAP"/>
     <parm name="ADDR" value="http://www.operator.com"/>
</characteristic>
```

OMA Data Synchronisation - “w5”

OMA Application Characteristic reference:

APPID: w5

APPID type: OMNA

Owner: Data Synchronisation Working Group

Contact: Data Synchronisation Working Group <OMA-DS@MAIL.OPENMOBILEALLIANCE.ORG>

Registration version: 1

Registration timestamp: 2004-01-09

Application description: Data Synchronisation (DS)

Application reference:

- OMA DS 1.2 specifications, http://www.openmobilealliance.org/release_program/ds_v12.html
- “SyncML Representation Protocol” specification, http://www.syncml.org/docs/syncml_represent_v111_20021002.pdf.

Description - “w5”

Creates a synchronisation account.

The settings for this application are grouped into accounts and maximum 5 accounts can be installed. An installed account is not overwritten, instead a new account is created.

Compliance

In the Usage column, the following abbreviations are used:
I = Ignored, M = Mandatory, N = Not used, and O = Optional.

Parameter	Usage	Description
Characteristic : APPLICATION		
APPID	M	“w5”
NAME	M	The name of the account
TO-NAPID	O	Reference to NAPDEF (data account). If value is "INTERNET" the default data account will be used
ADDR	(M)	The server address. Mandatory if APPLICATION:APPADDR:ADDR not set
APPLICATION : APPADDR	O	
ADDR	(M)	The server address. Mandatory if APPLICATION:ADDR not set
APPLICATION : APPAUTH	O	
AAUTHLEVEL	O	CLIENT **or** APPSRV. CLIENT means authentication data the client **receives** from the server. APPSRV means authentication data the client **sends** to the server. If no value is given AAUTH-LEVEL receives the value HTTP
AAUTHNAME	M	Username
AAUTHSECRET	M	User password
AAUTHDATA	O	
APPLICATION : RESOURCE	O	
URI	O	The database URI on the server
AACCEPT	O	Must be a MIME type supported by a database
AAUTHNAME	O	Username on database level
AAUTHSECRET	O	User password on database level

Example

```
<characteristic type="APPLICATION">
     <parm name="APPID" value="w5"/>
     <parm name="NAME" value="Scts"/>
     <parm name="TO-NAPID" value="INTERNET"/>
     <characteristic type="APPADDR">
          <parm name="ADDR" value="www.someserver.com:80/Sync"/>
     </characteristic>
     <characteristic type="APPAUTH">
          <parm name="AAUTHLEVEL" value="APPSRV"/>
          <parm name="AAUTHNAME" value="sync"/>
          <parm name="AAUTHSECRET" value="cnys"/>
     </characteristic>
     <characteristic type="APPAUTH">
          <parm name="AAUTHLEVEL" value="CLIENT"/>
          <parm name="AAUTHNAME" value="server"/>
          <parm name="AAUTHSECRET" value="revres"/>
          <parm name="AAUTHDATA" value="nonce"/>
     </characteristic>

     <characteristic type="APPAUTH">
          <parm name="AAUTHLEVEL" value="APPSRV"/>
          <parm name="AAUTHNAME" value="client"/>
          <parm name="AAUTHSECRET" value="teilc"/>
     </characteristic>
     <characteristic type="RESOURCE">
          <parm name="URI" value="pb"/>
          <parm name="AACCEPT" value="text/x-vcard,text/vcard"/>
          <parm name="AAUTHNAME" value="pb"/>
          <parm name="AAUTHSECRET" value="bp"/>
     </characteristic>
     <characteristic type="RESOURCE">
          <parm name="URI" value="cal"/>
          <parm name="AACCEPT" value="text/x-vcalendar"/>
          <parm name="AAUTHNAME" value="cal"/>
          <parm name="AAUTHSECRET" value="lac"/>
     </characteristic>
     <characteristic type="RESOURCE">
          <parm name="URI" value="notes"/>
          <parm name="AACCEPT" value="text/plain"/>
          <parm name="AAUTHNAME" value="notes"/>
          <parm name="AAUTHSECRET" value="seton"/>
     </characteristic>
     <characteristic type="RESOURCE">
          <parm name="URI" value="todo?TODO"/>
          <parm name="AACCEPT" value="text/x-vcalendar"/>
          <parm name="AAUTHNAME" value="todo"/>
          <parm name="AAUTHSECRET" value="odot"/>
     </characteristic>

     <characteristic type="RESOURCE">
          <parm name="URI" value="bkm"/>
          <parm name="AACCEPT" value="text/x-vbookmark"/>
          <parm name="AAUTHNAME" value="bkm"/>
          <parm name="AAUTHSECRET" value="mkb"/>
```

```
    </characteristic>

</characteristic>
```

OMA Device Management - “w7”

OMA Application Characteristic reference

APPID: w7

APPID type: OMNA

Owner: Device Management Working Group

Contact: Device Management Working Group <OMA-DM@MAIL.OPENMOBILEALLIANCE.ORG>

Registration version: 1

Registration timestamp: 2003-06-18

Application description: Device Management (DM)

Application reference:

- OMA Device Management, version 1.2 specifications, http://www.openmobilealliance.org/release_program/dm_v1_2.html
- “Device Management Tree and Description” specification, http://www.openmobilealliance.org/release_program/docs/CopyrightClick.asp?pck=DM&file=V1_2-20050628-C/OMA-TS-DM-TND-V1_2-20050615-C.pdf
- “Device Management Security” specification, http://www.openmobilealliance.org/release_program/docs/CopyrightClick.asp?pck=DM&file=V1_2-20060208-C/OMA-TS-DM-Security-V1_2-20060208-C.pdf
- “Device Management Representation Protocol” specification, http://www.openmobilealliance.org/release_program/docs/CopyrightClick.asp?pck=DM&file=V1_2-20051216-C/OMA-TS-DM-RepPro-V1_2-20051216-C.pdf

Description - “w7”

Creates a Device Management account.

The settings for this application are grouped into accounts and maximum 5 accounts can be installed. An installed account is not overwritten, instead a new account is created.

Compliance

In the Usage column, the following abbreviations are used:
I = Ignored, M = Mandatory, N = Not used, and O = Optional.

Parameter	Usage	Description
Characteristic : APPLICATION		
APPID	M	“w7”
PROVIDER-ID	M	Used as authentication name for the server. Max length 80. Must be unique among the installed Device Management accounts in the phone
INIT	O	Initiates a Device Management session after provisioning document has been installed. This parameter is an application specific parameter and is an extension
NAME	O	Used as displayable name in UI. Max length 50
TO-NAPID	M	Reference to NAPDEF (data account). If value is INTERNET default data account will be used
ADDR	(M)	Device Management server URI. Max length 255. Mandatory if APPLICATION:APPADDR:ADDR not set
APPLICATION : APPADDR	O	
ADDR	(M)	Device Management server URI. Mandatory if APPLICATION:ADDR not set
APPADDR : PORT	O	
PORTNBR	M	
APPLICATION : APPAUTH	O	There can be three APPAUTH within the APPLICATION characteristic. One for HTTP (if AAUTHLEVEL is missing), one for CLIENT and one for APPSRV
AAUTHLEVEL	O	CLIENT means authentication data the client **receives** from the server. APPSRV means authentication data the client **sends** to the server
AAUTHTYPE	O	Values can be HTTP-BASIC, HTTP-DIGEST (only valid if AAUTHLEVEL is missing), BASIC, DIGEST and/or HMAC. If multiple types are specified in a comma-separated list, there should be no white space before or after the commas
AAUTHNAME	O	Username. Max length 80
AAUTHSECRET	O	Password to use together with AAUTHNAME. Max length 60
AAUTHDATA	O	Used to specify nonce, Base64 encoded. Max length 52
Characteristic : EXT	O	Vendor specific tags
USEREDITABLE	O	Makes the DM account removable by default

Example

```
<characteristic type="APPLICATION">
     <parm name="APPID" value="w7"/>
     <parm name="PROVIDER-ID" value="serverId"/>
     <parm name="INIT"/>
     <parm name="NAME" value="Mgmt Server"/>
     <parm name="ADDR" value="http://www.mgmtserver.com:8080/
manage"/>
     <parm name="TO-NAPID" value="INTERNET"/>
     <characteristic type="APPAUTH">
          <parm name="AAUTHTYPE" value="HTTP-DIGEST"/>
          <parm name="AAUTHNAME" value="name"/>
          <parm name="AAUTHSECRET" value="secret"/>
     </characteristic>
     <characteristic type="APPAUTH">
          <parm name="AAUTHLEVEL" value="CLIENT"/>
          <parm name="AAUTHTYPE" value="DIGEST,BASIC"/>
          <parm name="AAUTHNAME" value="servername"/>
          <parm name="AAUTHSECRET" value="serversecret"/>
          <parm name="AAUTHDATA" value="c2VydmVybm9uY2U="/>
     </characteristic>
     <characteristic type="APPAUTH">
          <parm name="AAUTHLEVEL" value="APPSRV"/>
          <parm name="AAUTHNAME" value="clientname"/>
          <parm name="AAUTHSECRET" value="clientsecret"/>
          <parm name="AAUTHDATA" value="Y2xpZW50bm9uY2U="/>
     </characteristic>
     <characteristic type="EXT">
          <parm name="USEREDITABLE" value="1"/>
     </characteristic>
</characteristic>
```

Email, SMTP - “25”

OMA Application Characteristic reference

APPID: 25

APPID type: IANA

Owner: OMA DM Working Group

Contact: OMA DM Working Group <OMA-DM@MAIL.OPENMOBILEALLIANCE.ORG>

Registration version: 1

Registration timestamp: 2003-03-20

Application description: Email SMTP settings

Application reference: See RFC 2821 for SMTP definition

Description - “25”

Setting for the email SMTP (Simple Mail Transfer Protocol) server, that is, outgoing email.

Compliance

In the Usage column, the following abbreviations are used:
I = Ignored, M = Mandatory, N = Not used, and O = Optional.

Parameter	Usage	Description
Characteristic : APPLICATION		
APPID	M	“25”
PROVIDER-ID	O	Account name. Used to bind SMTP and POP3/IMAP4 settings together. Max length 20 characters
TO-NAPID	M	Reference to NAPDEF (data account). If value is INTERNET, default data account is used
ADDR	(M)	Outgoing server host name. Max length 31. Mandatory if APPLICATION:APPADDR:ADDR not set
FROM	O	User email address
APPLICATION : APPADDR	O	
ADDR	(M)	Outgoing server host name. Max length 31. Mandatory if APPLICATION:ADDR not set
APPADDR : PORT	O	
PORTNBR	O	Outgoing server port number. Default value is 25
SERVICE	O	Specifies secure protocol to be used. Possible value is START-TLS. All other values are ignored and the default is to not use secure protocol
APPLICATION : APPAUTH	O	
AAUTHNAME	M	Username for outgoing server. Max length 128
AAUTHSECRET	M	Password for incoming and outgoing server. Max length 40

Example

```
<characteristic type="APPLICATION">
  <parm name="APPID" value="25"/>
  <parm name="PROVIDER-ID" value="MyMail"/>
  <parm name="TO-NAPID" value="IAP1"/>
  <characteristic type="APPADDR">
    <parm name="ADDR" value="smtp.mail.com"/>
    <characteristic type="PORT">
      <parm name="PORTNBR" value="25"/>
      <parm name="SERVICE" value="STARTTLS"/>
    </characteristic>
  </characteristic>
  <characteristic type="APPAUTH">
    <parm name="AAUTHNAME" value="username"/>
    <parm name="AAUTHSECRET" value="password"/>
  </characteristic>
</characteristic>
```

Email, POP3 - “110”

OMA Application Characteristic reference

APPID: 110

APPID type: IANA

Owner: OMA DM Working Group

Contact: OMA DM Working Group <OMA-DM@MAIL.OPENMOBILEALLIANCE.ORG>

Registration version: 1

Registration timestamp: 2003-03-20

Application description: Email POP3 settings

Application reference: POP3 is defined in RFC1939.

Description - “110”

Setting for the incoming email server using POP3 protocol

Compliance

In the Usage column, the following abbreviations are used:
I = Ignored, M = Mandatory, N = Not used, and O = Optional.

Parameter	Usage	Description
Characteristic : APPLICATION		
APPID	O	“110”
PROVIDER-ID	O	Account name. Used to bind SMTP and POP3 settings together. Max length 20 characters
TO-NAPID	M	Reference to NAPDEF (data account). If value is INTERNET, default data account is used
ADDR	(M)	Incoming server host name. Max length 31 characters. Mandatory if APPLICATION:APPADDR:ADDR not set
APPLICATION : APPADDR	O	
ADDR	(M)	Incoming server host name. Max length 31 characters. Mandatory if APPLICATION:ADDR not set
APPADDR : PORT	O	
PORTNBR	O	Incoming server port number. 16-bit unsigned number
SERVICE	O	Specifies secure protocol to be used. Possible value is START-TLS. All other values are ignored and the default is to not use secure protocol
APPLICATION : APPAUTH	O	
AAUTHNAME	M	Incoming server username. Max length 128 characters
AAUTHSECRET	M	Incoming server password. Max length 40 characters

Example

```
<characteristic type="APPLICATION">
     <parm name="APPID" value="110"/>
     <parm name="PROVIDER-ID" value="MyMail"/>
     <parm name="TO-NAPID" value="IAP1"/>
     <characteristic type="APPADDR">
          <parm name="ADDR" value="pop.mail.com"/>
          <characteristic type="PORT">
               <parm name="PORTNBR" value="110"/>
               <parm name="SERVICE" value="STARTTLS"/>
          </characteristic>
     </characteristic>
     <characteristic type="APPAUTH">
          <parm name="AAUTHNAME" value="username"/>
          <parm name="AAUTHSECRET" value="password"/>
     </characteristic>
</characteristic>
```

Email, IMAP4 - “143”

OMA Application Characteristic reference

APPID: 143

APPID type: IANA

Owner: OMA DM Working Group

Contact: OMA DM Working Group <OMA-DM@MAIL.OPENMOBILEALLIANCE.ORG>

Registration version: 1

Registration timestamp: 2003-03-20

Application description: Email IMAP4 settings

Application reference: IMAP4 is defined in RFC2060

Description - “143”

This is the setting for the incoming email server using IMAP4 protocol.

Compliance

In the Usage column, the following abbreviations are used:
I = Ignored, M = Mandatory, N = Not used, and O = Optional.

Parameter	Usage	Description
Characteristic : APPLICATION		
APPID	M	“143”
PROVIDER-ID	O	Account name. Used to bind SMTP and IMAP4 settings together. Max 20 characters
TO-NAPID	M	Reference to NAPDEF (data account). If value is INTERNET, default data account is used
ADDR	(M)	Incoming server host name. Max length 31. Mandatory if APPLICATION:APPADDR:ADDR not set
APPLICATION : APPADDR	O	
ADDR	(M)	Incoming server host name. Max length 31. Mandatory if APPLICATION:ADDR not set
APPADDR : PORT	O	
PORTNBR	O	Incoming server port number. 16-bit unsigned number
SERVICE	O	Specifies secure protocol to be used. Possible value is START-TLS. All other values are ignored and the default is to not use secure protocol
APPLICATION : APPAUTH	O	
AAUTHNAME	M	Incoming server username. Max length 128
AAUTHSECRET	M	Incoming server password. Max length 40

Example

```
<characteristic type="APPLICATION">
  <parm name="APPID" value="143"/>
  <parm name="PROVIDER-ID" value="MyMail"/>
  <parm name="TO-NAPID" value="IAP1"/>
  <characteristic type="APPADDR">
    <parm name="ADDR" value="imap.mail.com"/>
    <characteristic type="PORT">
      <parm name="PORTNBR" value="143"/>
      <parm name="SERVICE" value="STARTTLS"/>
    </characteristic>
  </characteristic>
  <characteristic type="APPAUTH">
    <parm name="AAUTHNAME" value="username"/>
    <parm name="AAUTHSECRET" value="password"/>
  </characteristic>
</characteristic>
```

Streaming (3GPP) - “554”

OMA Application Characteristic reference

APPID: 554

APPID type: IANA

Owner: Device Management Working Group

Contact: Device Management Working Group <OMA-DM@MAIL.OPENMOBILEALLIANCE.ORG>

Registration version: 1

Registration timestamp: 2003-12-19

Application description: 3GPP PSS Streaming using Real Time Streaming Protocol (RTSP)

Application reference:

- 3GPP TS 26.234/www.3gpp.org/ftp/Specs/archive/26_series/26.234
- IETF (Internet Engineering Task Force) standards on streaming
- RTP (Real-time Transport Protocol)/RTCP (Real-time Transport Control Protocol) RFC1889/ www.ietf.org/rfc/rfc1889.txt
- RTSP (Real Time Streaming Protocol) RFC2326/www.ietf.org/rfc/rfc2326.txt
- SDP (Session Description Protocol) RFC2327/www.ietf.org/rfc/rfc2327.txt

Description - “554”

This is the setting for the streaming application.

New provisioned settings overwrite the old ones, but do not reset them.

Compliance

In the Usage column, the following abbreviations are used:
I = Ignored, M = Mandatory, N = Not used, and O = Optional.

Parameter	Usage	Description
Characteristic : APPLICATION		
APPID	M	“554”
TO-NAPID	M	Reference to NAPDEF (data account). If value is INTERNET default data account will be used

Example

```
<characteristic type="APPLICATION">
     <parm name="APPID" value="554"/>
     <parm name="TO-NAPID" value="INTERNET"/>
</characteristic>
```

IMPS(WV) - wA

Note: IMPS (WV) is **not** supported in phones with DM version 6.

OMA Application Characteristic reference

APPID: wA

APPID type: OMNA

Owner: OMA Instant Messaging and Presence Services Working Group

Contact: OMA IMPS WG <OMA-IMPS@MAIL.OPENMOBILEALLIANCE.ORG>

Registration version: 1

Registration timestamp: 2003-02-24

Application description: Instant Messaging and presence services (IMPS)

Application reference: None

Description - “wA”

The following settings are applicable to Wireless Village (“My Friends” in Sony Ericsson generic phones):

- UserID and Domain
- Password
- Server URL
- WAP Profile

When receiving an OMA Client Provisioning with Wireless Village settings, the currently active WV account is updated. New provisioned settings overwrite the old ones, but do not reset them.

Compliance

In the Usage column, the following abbreviations are used:
I = Ignored, M = Mandatory, N = Not used, and O = Optional.

Parameter	Usage	Description
Characteristic : APPLICATION		
APPID	M	“wA”
AACCEPT	O	Used to verify correct WV protocol version and XML coding (XML or WBXML)
TO-NAPID	M	Reference to NAPDEF (data account). If value is INTERNET the default data account will be used
ADDR	(M)	Address of WV server in URI form. Max 200 characters. Mandatory if APPLICATION:APPADDR:ADDR not set
APPLICATION : APPADDR	O	
ADDR	(M)	Address of WV server in URI form. Max 200 characters. Mandatory if APPLICATION:ADDR not set
ADDRTYPE	O	Only used to validate that ADDRTYPE is not “E164” (SMS bearer)
APPLICATION : APPAUTH	M	
AAUTHLEVEL	O	Only the value APPSRV is supported
AAUTHNAME	M	Complete WV UserID (including domain). Max 50 characters
AAUTHSECRET	M	Max 50 characters

Example

```
<characteristic type="APPLICATION">
  <parm name="APPID" value="wA"/>
  <parm name="AACCEPT" value="application/
vnd.wv.csp+xml;1.2;1.1;1.0,
application/vnd.wv.csp+wbxml;1.2;1.1;1.0"/>
  <parm name="ADDR" value="https://123.56.78.90"/>
  <parm name="ADDR" value="http://123.56.78.90"/>
  <characteristic type="APPAUTH">
     <parm name="AAUTHLEVEL" value="APPSRV"/>
     <parm name="AAUTHNAME" value="username"/>
     <parm name="AAUTHSECRET" value="password"/>
  </characteristic>
</characteristic>
```

Positioning – ap0004

OMA Application Characteristic reference

APPID: ap0004

APPID type: OMNA

Owner: OMA Location Working Group

Contact: OMA Location WG <TECHNICAL-COMMENTS@MAIL.OPENMOBILEALLIANCE.ORG>

Registration version: 1

Registration timestamp: 2005-04-12

Application description: Secure User Plane Location (SUPL)

Application reference: Secure User Plane Location (SUPL) OMA SUPL Enabler Release 1.0 specifications. http://www.openmobilealliance.org/documents.asp

Description - “ap0004”

Sets Home SUPL Location Platform (H-SLP) server address.

New provisioned settings overwrite the old ones, but do not reset them.

Compliance

In the Usage column, the following abbreviations are used:
I = Ignored, M = Mandatory, N = Not used, and O = Optional.

Parameter	Usage	Description
Characteristic : APPLICATION		
APPID	M	"ap0004"
ADDR	M	Address of the H-SLP server

IP Multimedia Subsystem (IMS) – ap2001

Note: IMS is **not** supported in phones with DM version 6.

OMA Application Characteristic reference

APPID: ap2001

APPID type: OMNA

Owner: 3GPP CT1 Working Group

Contact: 3GPP TSG CT WG1

Registration version: 1.0

Registration timestamp: 2005-xx-xx

Application description: IP Multimedia Subsystem (IMS)

Application reference: IMS specifications, TS 24.229, 23.221 and 23.228.
http://ftp.3gpp.org/

Description - “ap2001”

Settings for IP Multimedia Subsystem (IMS).

New provisioned settings overwrite the old ones, but do not reset them.

Compliance

In the Usage column, the following abbreviations are used:
I = Ignored, M = Mandatory, N = Not used, and O = Optional.

Parameter	Usage	Description
Characteristic : APPLICATION		
APPID	M	“ap2001”
NAME	O	Account name
TO-NAPID	M	Reference to NAPDEF (data account). If value is INTERNET, default data account will be used
PDP_CONTEXTOPERPREF	I	Dedicated PDP context for SIP signalling is currently not supported
P-CSCF_ADDRESS	O	Defines an FQDN to an IPv4 P-CSCF. Shall only be used in early IMS implementations as described in 3GPP TS 23.221
TIMER_T1	O	Round trip time given in milliseconds
TIMER_T2	O	Maximum retransmit interval for non-INVITE requests and INVITE responses given in milliseconds
TIMER_T4	O	Maximum duration a message will remain in the network given in milliseconds
Characteristic : EXT		Sony Ericsson IMS-client specific parameters

In the Usage column, the following abbreviations are used:
I = Ignored, M = Mandatory, N = Not used, and O = Optional.

Parameter	Usage	Description
PROFILE_MODE	O	Accepted values: • "IETF" • "IMS" Default profile mode is IMS
ISIM_MANDATORY_FLAG	O	“0” indicates that the use of an ISIM is not mandatory. “1” indicates that the use of an ISIM is mandatory. Default value: 0
TRANSPORT	O	Transport protocol used between UE and proxy. Accepted values are “UDP” and “TCP”. Default protocol is UDP
LOOSE_ROUTER	O	“0” indicates that loose routing is disabled. “1” indicates that loose routing is enabled. Loose routing is enabled per default
REGISTRATION_EVENTS	O	“0” indicates that subscriptions for registration events like network initiated deregistration or reauthentication after successful registration are disabled. “1” indicates that subscriptions for registration events like network initiated deregistration or reauthentication after successful registration are enabled. Subscriptions are enabled per default
TIMER_CLIENT_TRANSACTION	O	Maximum lifetime for a SIP client transaction in milliseconds. Default value is 180000 (that is, 3 minutes)
REALM	O/M	Realm to use for authentication (IETF mode only)
REALM_USER_NAME	O/M	Realm username to use for authentication (IETF mode only)
REALM_USER_PASSWORD	O/M	Realm user password to use for authentication (IETF mode only)
SIGNAL_COMP	O	“0” indicates that signal compression should not be used. ”1” indicates that signal compression should be used. Default value: 0
SESSION_TIMER	O	Session expiry timer value given in seconds. If value is “0” the session expiry timer is deactivated. Default value is 1800 and the smallest accepted expiry timer value is 90

In the Usage column, the following abbreviations are used: *I = Ignored, M = Mandatory, N = Not used, and O = Optional.*		
Parameter	**Usage**	**Description**
PROXY_PORT	O	Proxy port used in Early IMS implementations. Default value is 5060
AUTHENTICATION_MODE	O	Allows the provider to specify the type of authentication support they provide. Accepted values are: • “EARLY_IMS” • “FULL_IMS” • “FALLBACK” “FALLBACK” has the effect that if “FULL_IMS” authentication fails, “EARLY_IMS” will be tried as well. Default value is “FULL_IMS”

Example

```
<characteristic type="APPLICATION">
     <parm name="APPID" value="ap2001" />
     <parm name="NAME" value="IMS-account" />
     <parm name="APPREF" value="IMS1" />
     <parm name="TO-NAPID" value="INTERNET" />
     <parm name="PDP_CONTEXTOPERPREF" value="0" />
     <parm name="P-CSCF_ADDRESS" value="address.com" />
     <parm name="TIMER_T1" value="1000" />
     <parm name="TIMER_T2" value="1100" />
     <parm name="TIMER_T4" value="1200" />
     <characteristic type="EXT">
          <parm name="PROFILE_MODE" value="IETF" />
          <parm name="SIGNAL_COMP" value="1" />
          <parm name="SESSION_TIMER" value="1500" />
          <parm name="PROXY_PORT" value="5050" />
          <parm name="TRANSPORT" value="TCP" />
          <parm name="ISIM_MANDATORY_FLAG" value="1" />
          <parm name="REGISTRATION_EVENTS" value="0" />
          <parm name="LOOSE_ROUTER" value="0" />
          <parm name="TIMER_CLIENT_TRANSACTION" value="170000" />
          <parm name="AUTHENTICATION_MODE" value="EARLY_IMS" />
          <parm name="REALM" value="operator-realm.com" />
          <parm name="REALM_USER_NAME" value="username" />
          <parm name="REALM_USER_PASSWORD" value="passwd" />
     </characteristic>
</characteristic>
```

Sony Ericsson MobileTV – x-semc-mobile-tv

Note: This application is only implemented in C702, C902, C905, T700, W595, W760, W902, W980, Z770 and Z780 phones.

OMA Application Characteristic reference

APPID: x-semc-mobile-tv

APPID type: Sony Ericsson proprietary

Owner: Sony Ericsson

Contact: Sony Ericsson

Registration version: N/A

Registration timestamp: N/A

Application description: Sony Ericsson Mobile TV

Application reference: N/A

Description - "x-semc-mobile-tv"

Settings for Sony Ericsson MobileTV.

New provisioned settings overwrite the old ones, but do not reset them.

Compliance

In the Usage column, the following abbreviations are used:
I = Ignored, M = Mandatory, N = Not used, and O = Optional.

Parameter	Usage	Description
Characteristic : APPLICATION		
APPID	M	"x-semc-mobile-tv"
DSL-SERVER-URL	M	The URL of the OPML file. Max 512 characters. Max 10 URLs
MIN-UPDATE-INTERVAL	O	Sets the maximum time that can elapse between client updates. Measured in minutes. Default value is 1440
ECDS-SERVER-URL	M	The ECDS server URL. Max 512 characters

Example

```
<characteristic type="APPLICATION">
     <parm name="APPID" value="x-semc-mobile-tv" />
     <parm name="DSL-SERVER-URL" value="dsladdress1.com" />
     <parm name="DSL-SERVER-URL" value="dsladdress2.com" />
     <parm name="DSL-SERVER-URL" value="dsladdress3.com" />
     <parm name="MIN-UPDATE-INTERVAL" value="1441" />
     <parm name="ECDS-SERVER-URL" value="ecdsserver.com" />
</characteristic>
```

Generic Access Network (GAN) – x-semc-gan-service

OMA Application Characteristics reference

APPID: x-semc-gan-service

APPID type: Sony Ericsson proprietary

Owner: Sony Ericsson

Contact: Sony Ericsson

Registration version: N/A

Registration timestamp: N/A

Application description: Sony Ericsson GAN service

Application reference: N/A

Description - "x-semc-gan-service"

Settings for Sony Ericsson GAN service.

New provisioned settings overwrite the old ones.

Compliance

In the Usage column, the following abbreviations are used:
I = Ignored, M = Mandatory, N = Not used, and O = Optional.

Parameter	Usage	Description
Characteristic : APPLICATION	O	
APPID	M	"x-semc-gan-service"
PGANC	M	The FQDN (Fully Qualified Domain Name) address of the provisioning gan controller
PSEGW	M	The FQDN (Fully Qualified Domain Name) address of the provisioning security gateway

Example

```
<wap-provisioningdoc version="1.1">
     <characteristic type="APPLICATION">
          <parm name="APPID" value="x-semc-gan-service"/>
          <parm name="PGANC" value="pganc.sonyericsson.com"/>
          <parm name="PSEGW" value="psegw.sonyericsson.com"/>
     </characteristic>
</wap-provisioningdoc>
```

General client provisioning examples

Settings for Browsing (w2) HTTP protocol, MMS (w4), OMA Data Synchronisation (w5) and OMA Device Management (w7).

```
<?xml version="1.0"?>
<!DOCTYPE wap-provisioningdoc PUBLIC "-//WAPFORUM//DTD PROV 1.0/
/EN" "http://www.wapforum.org/DTD/prov.dtd">
<wap-provisioningdoc version="1.1">
     <characteristic type="BOOTSTRAP">
          <parm name="PROVURL" value="https://operator"/>
          <parm name="NAME" value="Operator Settings"/>
     </characteristic>

     <characteristic type="PXLOGICAL">
          <parm name="PROXY-ID" value="webproxy.operator.com"/>
          <parm name="NAME" value="Not used"/>
          <characteristic type="PXPHYSICAL">
               <parm name="PHYSICAL-PROXY-ID" value="proxy 1"/>
               <parm name="PXADDR" value="webproxy.operator.com"/
>
               <parm name="PXADDRTYPE" value="ALPHA"/>
               <parm name="TO-NAPID" value="web.operator.com"/>
               <characteristic type="PORT">
                    <parm name="PORTNBR" value="8080"/>
               </characteristic>
          </characteristic>
     </characteristic>

     <characteristic type="PXLOGICAL">
          <parm name="PROXY-ID" value="mmsproxy.operator.com"/>
          <parm name="NAME" value="Not used"/>
          <characteristic type="PXPHYSICAL">
               <parm name="PHYSICAL-PROXY-ID" value="Operator
MMS"/>
               <parm name="PXADDR" value="mmsproxy.operator.com"/
>
               <parm name="PXADDRTYPE" value="ALPHA"/>
               <parm name="TO-NAPID" value="mms.operator.com"/>
               <characteristic type="PORT">
                    <parm name="PORTNBR" value="8080"/>
               </characteristic>
          </characteristic>
     </characteristic>

     <characteristic type="NAPDEF">
          <parm name="NAPID" value="web.operator.com"/>
          <parm name="BEARER" value="GSM-GPRS"/>
          <parm name="NAME" value="Operator Web"/>
          <parm name="NAP-ADDRESS" value="web.operator.com"/>
          <parm name="NAP-ADDRTYPE" value="APN"/>
          <characteristic type="NAPAUTHINFO">
               <parm name="AUTHTYPE" value="PAP"/>
```

```
                <parm name="AUTHNAME" value="webuser"/>
                <parm name="AUTHSECRET" value="webpasswd"/>
           </characteristic>
     </characteristic>

     <characteristic type="NAPDEF">
           <parm name="NAPID" value="mms.operator.com"/>
           <parm name="BEARER" value="GSM-GPRS"/>
           <parm name="NAME" value="Operator MMS"/>
           <parm name="NAP-ADDRESS" value="mms.operator.com"/>
           <parm name="NAP-ADDRTYPE" value="APN"/>
           <characteristic type="NAPAUTHINFO">
                <parm name="AUTHTYPE" value="PAP"/>
                <parm name="AUTHNAME" value="mmsuser"/>
                <parm name="AUTHSECRET" value="mmspasswd"/>
           </characteristic>
     </characteristic>


     <characteristic type="APPLICATION">
           <parm name="APPID" value="w2"/>
           <parm name="TO-NAPID" value="web.operator.com" />
           <characteristic type="RESOURCE">
                <parm name="URI" value="www.operator.com/"/>
                <parm name="NAME" value="Some Operator WAP
Service"/>
                <parm name="STARTPAGE"/>
           </characteristic>
           <characteristic type="RESOURCE">
                <parm name="URI" value="www.somewhere.com/ "/>
                <parm name="NAME" value="Bookmark 1"/>
           </characteristic>
           <characteristic type="RESOURCE">
                <parm name="URI" value="www.nowhere.com/ "/>
                <parm name="NAME" value="Bookmark 2"/>
           </characteristic>
     </characteristic>


     <characteristic type="APPLICATION">
           <parm name="APPID" value="w4"/>
           <parm name="TO-NAPID" value="mms.operator.com"/>
           <parm name="ADDR" value="http://mms.operator.com"/>
     </characteristic>


     <characteristic type="APPLICATION">
           <parm name="APPID" value="w5"/>
           <parm name="NAME" value="Sync service"/>
           <parm name="TO-NAPID" value="web.operator.com"/>
           <characteristic type="APPADDR">
                <parm name="ADDR" value="www.someserver.com:80/
Sync"/>
           </characteristic>
           <characteristic type="APPAUTH">
```

```
                <parm name="AAUTHLEVEL" value="APPSRV"/>
                <parm name="AAUTHNAME" value="sync"/>
                <parm name="AAUTHSECRET" value="cnys"/>
           </characteristic>
           <characteristic type="APPAUTH">
                <parm name="AAUTHLEVEL" value="CLIENT"/>
                <parm name="AAUTHNAME" value="client"/>
                <parm name="AAUTHSECRET" value="teilc"/>
           </characteristic>
           <characteristic type="RESOURCE">
                <parm name="URI" value="pb"/>
                <parm name="AACCEPT" value="text/x-vcard,text/
vcard"/>
                <parm name="AAUTHNAME" value="pb"/>
                <parm name="AAUTHSECRET" value="bp"/>
           </characteristic>
           <characteristic type="RESOURCE">
                <parm name="URI" value="cal"/>
                <parm name="AACCEPT" value="text/x-vcalendar"/>
                <parm name="AAUTHNAME" value="cal"/>
                <parm name="AAUTHSECRET" value="lac"/>
           </characteristic>
           <characteristic type="RESOURCE">
                <parm name="URI" value="notes"/>
                <parm name="AACCEPT" value="text/plain"/>
                <parm name="AAUTHNAME" value="notes"/>
                <parm name="AAUTHSECRET" value="seton"/>
           </characteristic>
           <characteristic type="RESOURCE">
                <parm name="URI" value="todo?TODO"/>
                <parm name="AACCEPT" value="text/x-vcalendar"/>
                <parm name="AAUTHNAME" value="todo"/>
                <parm name="AAUTHSECRET" value="odot"/>
           </characteristic>
           <characteristic type="RESOURCE">
              <parm name="URI" value="bkm"/>
              <parm name="AACCEPT" value="text/x-vbookmark"/>
              <parm name="AAUTHNAME" value="bkm"/>
              <parm name="AAUTHSECRET" value="mkb"/>
        </characteristic>
      </characteristic>


      <characteristic type="APPLICATION">
           <parm name="APPID" value="w7"/>
           <parm name="PROVIDER-ID" value="mgmtserver.com"/>
           <parm name="NAME" value="Mgmt Server"/>
           <parm name="ADDR" value="http://
www.mgmtserver.com:8080/manage"/>
           <parm name="TO-NAPID" value="web.operator.com" />
           <characteristic type="APPAUTH">
                <parm name="AAUTHNAME" value="httpuser"/>
                <parm name="AAUTHSECRET" value="httpsecret"/>
           </characteristic>
           <characteristic type="APPAUTH">
```

```
            <parm name="AAUTHLEVEL" value="APPSRV"/>
            <parm name="AAUTHNAME" value="clientname"/>
            <parm name="AAUTHSECRET" value="clientsecret"/>
            <parm name="AAUTHDATA" value="Y2xpZW50bm9uY2U="/>
        </characteristic>
        <characteristic type="APPAUTH">
            <parm name="AAUTHLEVEL" value="CLIENT"/>
            <parm name="AAUTHNAME" value="servername"/>
            <parm name="AAUTHSECRET" value="serversecret"/>
            <parm name="AAUTHDATA" value="c2VydmVybm9uY2U="/>
        </characteristic>
    </characteristic>
</wap-provisioningdoc>
```

Settings for Email POP3 (110) and Email SMTP (25)

```
<?xml version="1.0"?>
<!DOCTYPE wap-provisioningdoc PUBLIC "-//WAPFORUM//DTD PROV 1.0/
/EN"
"http://www.wapforum.org/DTD/prov.dtd">

<wap-provisioningdoc version="1.1">

  <characteristic type="NAPDEF">
     <parm name="NAPID" value="operator.com"/>
     <parm name="BEARER" value="GSM-GPRS"/>
     <parm name="NAME" value="Operator GPRS"/>
     <parm name="NAP-ADDRESS" value="mailweb.operator.com"/>
     <parm name="NAP-ADDRTYPE" value="APN"/>
     <characteristic type="NAPAUTHINFO">
       <parm name="AUTHTYPE" value="PAP"/>
       <parm name="AUTHNAME" value="user"/>
       <parm name="AUTHSECRET" value="passwd"/>
     </characteristic>
  </characteristic>

  <characteristic type="APPLICATION">
    <parm name="APPID" value="110"/>
    <parm name="PROVIDER-ID" value="MyMail"/>
    <parm name="TO-NAPID" value="operator.com"/>
    <characteristic type="APPADDR">
      <parm name="ADDR" value="pop.mail.com"/>
      <characteristic type="PORT">
        <parm name="PORTNBR" value="110"/>
        <parm name="SERVICE" value="STARTTLS"/>
      </characteristic>
    </characteristic>
    <characteristic type="APPAUTH">
      <parm name="AAUTHNAME" value="username"/>
      <parm name="AAUTHSECRET" value="password"/>
    </characteristic>
  </characteristic>

  <characteristic type="APPLICATION">
    <parm name="APPID" value="25"/>
    <parm name="PROVIDER-ID" value="MyMail"/>
```

```
    <parm name="TO-NAPID" value="operator.com"/>
    <characteristic type="APPADDR">
      <parm name="ADDR" value="smtp.mail.com"/>
      <characteristic type="PORT">
        <parm name="PORTNBR" value="25"/>
        <parm name="SERVICE" value="STARTTLS"/>
      </characteristic>
    </characteristic>
    <characteristic type="APPAUTH">
      <parm name="AAUTHNAME" value="username"/>
      <parm name="AAUTHSECRET" value="password"/>
    </characteristic>
  </characteristic>

</wap-provisioningdoc>
```

Settings for Email IMAP4 (143) and Email SMTP (25)

```
<?xml version="1.0"?>
<!DOCTYPE wap-provisioningdoc PUBLIC "-//WAPFORUM//DTD PROV 1.0/
/EN"
"http://www.wapforum.org/DTD/prov.dtd">

<wap-provisioningdoc version="1.1">

  <characteristic type="NAPDEF">
     <parm name="NAPID" value="operator.com"/>
     <parm name="BEARER" value="GSM-GPRS"/>
     <parm name="NAME" value="Operator GPRS"/>
     <parm name="NAP-ADDRESS" value="mailweb.operator.com"/>
     <parm name="NAP-ADDRTYPE" value="APN"/>
     <characteristic type="NAPAUTHINFO">
       <parm name="AUTHTYPE" value="PAP"/>
       <parm name="AUTHNAME" value="user"/>
       <parm name="AUTHSECRET" value="passwd"/>
     </characteristic>
  </characteristic>

<characteristic type="APPLICATION">
    <parm name="APPID" value="143"/>
    <parm name="PROVIDER-ID" value="MyMail"/>
    <parm name="TO-NAPID" value="operator.com"/>
    <characteristic type="APPADDR">
      <parm name="ADDR" value="imap.mail.com"/>
      <characteristic type="PORT">
        <parm name="PORTNBR" value="143"/>
        <parm name="SERVICE" value="STARTTLS"/>
      </characteristic>
    </characteristic>
    <characteristic type="APPAUTH">
      <parm name="AAUTHNAME" value="username"/>
      <parm name="AAUTHSECRET" value="password"/>
    </characteristic>
  </characteristic>
```

```
  <characteristic type="APPLICATION">
    <parm name="APPID" value="25"/>
    <parm name="PROVIDER-ID" value="MyMail"/>
    <parm name="TO-NAPID" value="operator.com"/>
    <characteristic type="APPADDR">
      <parm name="ADDR" value="smtp.mail.com"/>
      <characteristic type="PORT">
        <parm name="PORTNBR" value="25"/>
        <parm name="SERVICE" value="STARTTLS"/>
      </characteristic>
    </characteristic>
    <characteristic type="APPAUTH">
      <parm name="AAUTHNAME" value="username"/>
      <parm name="AAUTHSECRET" value="password"/>
    </characteristic>
  </characteristic>

</wap-provisioningdoc>
```

WBXML client provisioning document example

This example illustrates the encoding of a XML client provisioning document into WBXML format.

XML format

```
<wap-provisioningdoc version="1.1">
     <characteristic type="APPLICATION">
          <parm name="NAME" value="DM-account" />
          <parm name="APPID" value="w7" />
          <parm name="PROVIDER-ID" value="provider id" />
          <parm name="INIT"/>
          <parm name="TO-PROXY" value="px1" />
          <characteristic type="APPADDR">
               <parm name="ADDR" value="www.serveraddress.com" />
               <characteristic type="PORT">
                    <parm name="PORTNBR" value="8080" />
               </characteristic>
          </characteristic>
          <characteristic type="APPAUTH">
               <parm name="AAUTHLEVEL" value="CLIENT" />
               <parm name="AAUTHTYPE" value="BASIC,DIGEST" />
               <parm name="AAUTHNAME" value="clientname" />
               <parm name="AAUTHSECRET" value="clientpw" />
               <parm name="AAUTHDATA" value="Y2xpZW50bm9uY2U=" />
          </characteristic>
```

```
          <characteristic type="APPAUTH">
               <parm name="AAUTHLEVEL" value="APPSRV" />
               <parm name="AAUTHTYPE" value="BASIC" />
               <parm name="AAUTHSECRET" value="serverpw" />
               <parm name="AAUTHDATA" value="c2VydmVybm9uY2U=" />
          </characteristic>
     </characteristic>
</wap-provisioningdoc>
```

WBXML encoding

Token stream	Description
01	Transaction ID
06	PDU Type: Push
2F	Header length
1F	Value length, *long* indicator
2D	Value length
B6	Media type. Assigned number for application/vnd.wap.connectivity-wbxml (0x36) encoded as short integer (0x80)
91	SEC parameter
81	Security method USERPIN (0x01) encoded as short integer (0x80)
92	MAC parameter (0x12) encoded as short integer (0x80)
45 35 38 35 37 46 32 39 30 36 35 44 43 32 34 34 39 43 32 33 46 43 46 45 46 33 44 35 44 37 36 33 46 39 34 30 30 35 44 44	MAC value is "E5857F29065DC2449C23FCFEF3D5D763F94005DD", associated PIN is 1234
00	End of string for the encoded MAC value
03	WBXML version 1.3
0B	Document Public Identifier: "-//WAPFORUM//DTD PROV 1.0//EN"
6A	Character set UTF-8
00	String table length
C5	Element <wap-provisioningdoc> includes attribute and content
45	Attribute version...
03	...encoded as inline string:
31 2E 31	"1.1"
00	End of string
01	End of attribute list

Token stream	Description
C6	Characteristic…
00 01	Code page switch (0x00) to code page (0x01)
55	...APPLICATION (0x55 at code page 1)
01	End of attribute list
87	Parameter…
00 00	Code page switch (0x00) to code page 0
07 06 03 44 4D 2D 61 63 63 6F 75 6E 74 00 01	...NAME carrying the inline string "DM-account"
87 00 01 36 00 00 06 03 77 37 00 01	Parameter APPID (0x36 at code page 1) carrying the inline string "w7"
87 00 01 38 00 00 06 03 70 72 6F 76 69 64 65 72 20 69 64 00 01	Parameter PROVIDER-ID carrying the inline string "provider id"
87 05 03 49 4E 49 54 00 01	Parameter with name (0x05) defined by inline string (0x03) "INIT"
87 00 01 39 00 00 06 03 70 78 31 00 01	Parameter TO-PROXY carrying the inline string "px1"
C6 00 01 56 01	Characteristic APPADDR
87 34 00 00 06 03 77 77 77 2E 73 65 72 76 65 72 61 64 64 72 65 73 73 2E 63 6F 6D 00 01	Parameter ADDR carrying the inline string "www.serveraddress.com"
C6 53 01	Characteristic PORT
87 23 06 03 38 30 38 30 00 01	Parameter PORTNBR carrying the inline string 8080
01	End of characteristic PORT
01	End of characteristic APPADDR
C6 00 01 57 01	Characteristic APPAUTH
87 30 00 00 06 03 43 4C 49 45 4E 54 00 01	Parameter AAUTHLEVEL carrying the inline string "CLIENT"
87 00 01 33 00 00 06 00 01 92 90 93 01	Parameter AAUTHTYPE carrying the values BASIC,DIGEST
87 31 00 00 06 03 63 6C 69 65 6E 74 6E 61 6D 65 00 01	Parameter AAUTHNAME carrying the inline string "clientname"
87 00 01 32 00 00 06 03 63 6C 69 65 6E 74 70 77 00 01	Parameter AAUTHSECRET carrying the inline string "clientpw"

Token stream	Description
87 00 01 2F 00 00 06 03 59 32 78 70 5A 57 35 30 62 6D 39 75 59 32 55 3D 00 01	Parameter AAUTHDATA carrying the inline string "Y2xpZW50bm9uY2U=" (“clientnonce” B64 encoded)
01	End of characteristic APPAUTH
C6 00 01 57 01	Characteristic APPAUTH
87 30 00 00 06 00 01 8D 01	Parameter AAUTHLEVEL carrying the value APPSRV
87 33 00 00 06 00 01 92 01	Parameter AAUTHTYPE carrying the value BASIC
87 32 00 00 06 03 73 65 72 76 65 72 70 77 00 01	Parameter AAUTHSECRET carrying the inline string "serverpw"
87 00 01 2F 00 00 06 03 63 32 56 79 64 6D 56 79 62 6D 39 75 59 32 55 3D 00 01	Parameter AAUTHDATA carrying the inline string "c2VydmVybm9uY2U=" (“servernonce” B64 encoded)
01	End of characteristic APPAUTH
01	End of characteristic APPLICATION
01	End of element <wap-provisioningdoc>, that is, end of provisioning document

OMA Device Management

OMA Device Management offers an advanced method for centralised control and management of different configuration settings in devices. Device Management is carried out in sessions where a management server, through a dialogue with the mobile device client, updates one or several configuration settings in the device. For example, the server can install new or upgraded applications, update settings for Internet, MMS and email, and install new themes in a phone.

Introduction

OMA Device Management is based on the same technology as OMA Data Synchronisation (formerly known as SyncML Data Synchronisation). The main difference is that, while OMA DS synchronises two or more sets of data in two or more devices, OMA Device Management updates client device configuration settings from data stored on one specific server.

The Client Provisioning and Device Management technologies are also based on similar technologies. One important difference between the technologies is the communication between server and client:

- Client Provisioning is performed in a one-way communication where the server sends a provisioning document to the client. The XML content of the file is parsed and the settings contained in the document are stored in the client device. There is no dialogue between the client and server after data transfer has started.

- Device Management is carried out in sessions. Once a session is established, the server sends one or several WBXML encoded commands to the client, and the client responds to each command with result and status information. (The protocol allows either XML or WBXML encoding, but Sony Ericsson clients only support WBXML.)

In Device Management client devices, data that can be affected by Device Management activities are stored in a tree structure defined in OMA standards. The DM tree contains nodes and leaves. Leaves contain settings and parameter values, controlling software and hardware operations in the device. Leaves are always on the lowest level in the DM tree and cannot therefore contain any sublevels. Groups of settings and parameters for a specific application are referred to as Management Objects (MO) and are represented as “branches” of the DM tree. In this way an MO is found as a number of subnodes and leaves emanating from one node.

Dynamic nodes are nodes and leaves that can be added by a DM server using the *Add* command. The DDF often uses the Occurrence tag to indicate whether a particular node is an important (Occurrence One), or more optional (Occurence ZeroOrOne), setting within an MO. That is, it is generally recommended that the server explicitly adds nodes with Occurrence One while optional nodes may be omitted. The Sony Ericsson DM client, however, implicitly creates missing nodes in newly added MOs, after the DM session ends. Therefore, when the server reconnects to the phone in a subsequent DM session, the existing MOs are complete. If the server wants to modify the values of any leaves, it now has to use the *Replace* command.

DM *Delete* command is usually not allowed on single nodes within an MO, to ensure the integrity of, for example, account structures. In many cases dynamic MOs can be deleted at the placeholder level instead.

Device Management is typically implemented in a phone as follows:

1. OMA Client Provisioning is used to bootstrap the phone with settings for an OMA DM account.

2. OMA DM sessions are initiated using the built-in security and authentication features.

3. During DM sessions the accounted server sends WBXML-encoded commands to the client, and the client responds to these with results and status information. Data in the DM tree can be read, changed or deleted, or new data can be stored in the tree.

4. Programmatically, DM sessions are always initiated by the client, but a DM server may alert the client about recommended DM activities. In this way, a DM use case can be regarded as initiated by either the phone (DM client) or by the DM server.

Supported standards and protocols

OMA Device Management has its origin in SyncML DM and has been standardised by OMA. See the following documents, found at http://www.openmobilealliance.org/ for details of the standards:

- Device Management Tree and Description version 1.2
- Device Management Protocol version 1.2
- Device Management Representation Protocol version 1.2
- Device Management Security version 1.2
- Device Management Bootstrap, version 1.2
- Device Management Standardised Objects, version 1.2
- Notification Initiated Session, version 1.2

Preconditions

Common preconditions for DM sessions to take place are:

- The client (phone) has a correctly configured DM and data account.

- The client is registered in a GSM/UMTS network, to be able to receive connectionless WAP push (SMS).

- The client can connect/be connected, typically via HTTP with bearers GSM/GPRS or packet-switched WCDMA.

DM sessions

A DM session can be divided into two phases:

- The setup phase, in which authentication and device information exchange takes place between the client and server.

- The management phase, in which management actions are carried out in an iterated process. The Device Management server sends DM commands in WBXML format to the client, and the client responds with messages containing Results and/or Status values. The server finally sends a message with no operations, to which the client manager responds by finalising the DM session.

For detailed information about the different types of messages needed to carry out sessions, see *SyncML Device Management Protocol version 1.2*, http://www.openmobilealliance.org/

General use case

A Device Management session is set up between a phone and a DM server. The server intends to configure the phone and/or to read information from it. In this use case it is assumed that the server takes the initiative to the session, and that the phone (and possibly its user) responds to the server initiative.

A DM server decides that it wants to establish a DM session to perform a certain task. The decision can be made automatically, for example, via a timer event controlled by parameter settings or ordered by a server operator.

Example: An operator is launching a new service and, as a result of this, is restructuring its service network, requiring some existing customers to modify their configurations.

1. The DM server sends out a package 0 message using connectionless WAP push. (See *Notification Initiated Session* for details on the standard).

2. The message is received and its integrity checked in the phone.

3. Depending on internal settings in the DM account, the package 0 push is handled according to one of the following directives:

    - *Accept*. The client accepts the package 0 message automatically and starts the DM session without user interaction. However, if <ui-mode> in the message is set to “user interaction” by the server, the user is prompted as in the *Always ask* alternative below.
    - *Never accept*. The client is set to reject all package 0 messages on the current DM account. This ends the use case automatically.
    - *Always ask*. The user is prompted (yes/no) to accept the DM session or not. The use case continues if the user answers yes.

4. The phone establishes the session. The phone displays that an activity is ongoing and the DM session continues.

5. During the session the DM server writes and reads application data to/from the phone.

6. When the DM server has finished its task, it terminates the DM session by sending an empty package to the phone. The session ends.

Versioning

The following table lists Device Management client and protocol versions implemented in Sony Ericsson phones. **Note:** This document only covers DM clients versions 5.0 and 6.0. Earlier versions are covered in two other Developers guidelines documents found at Sony Ericsson Developer World.

Device Management		Implemented in
client version	protocol version	
1.0	1.1.2	K600, K750, V600, W700, W800 and Z525 series
2.0	1.1.2	K310, K320, K510, W200, W300, W550, W600, W810, W900, Z530, Z550 and Z558 series
3.0	1.2	K550 (except K550im), K610 (except K610im), K790, K800, K810, W610, W660, W710, W830, W850, W880, Z610 and Z710 series
3.1	1.2	W380 and Z310 series
3.2	1.2	K610im and K550im phone models (i-mode phones)
3.3	1.2	K530, K770 and T650 series
4.0	1.2	K630, K850, V640, W910 and Z750 series
4.1	1.2	K660 and W890 series
4.2	1.2	C702, C902, T700, W595, W760, W902, W980, Z770 and Z780 series
5.0	1.2	C510, C901, C903, C905, G705, Jalou™, Naite™, T707, T715, W508, W705, W715 and W995 series
6.0	1.2	Aino™, Cedar, Elm, Hazel, Pureness™, Yari™ and Zylo series

The DevInfo/DmV node contains the version number of the Device Management client implementation, as specified in the table. For example, the DM client in C905 series is version 5.0.

Minor version increments indicate small changes, for example, addition of a new management object or minor changes to existing nodes (such as a changed Format or AccessType for a node).

Major version increments indicates a new generation of the DM client software, which usually also means changes to the DM tree structure or some new or extended management objects.

Every increment in the DmV value mandates the release of a new corresponding DDF on the Sony Ericsson Web site. The URL to Sony Ericsson online DDFs is wap.sonyericsson.com/ddf/<filename>.xml

The appropriate value of <filename> is constructed by concatenating the value of the DmV node in the phone with the prefix string "sonyericsson_ddf_".

Example:

A C905 phone has a DmV value of 5.0 and the corresponding DDF can be found at wap.sonyericsson.com/ddf/sonyericsson_ddf_5.0.xml.

Authentication

The OMA Device Management standard defines two different security mechanisms: transport security and protocol security. Protocol security includes all authentication mechanisms defined in the DM standard, for example, Basic, MD5 and HMAC mechanisms.

In Sony Ericsson DM clients, transport security is handled by using a HTTP connection with TLS/SSL when URLs begin with "https:". If a DM account is specified to use transport security (that is, its server URL begins with "https:"), the DM server is regarded as authenticated from start and the client does not send any protocol challenge to the server. However, the client still responds to any protocol challenges from the server.

The DM client keeps track internally of the latest authentication mechanism used by the server and sends corresponding credentials in the first client package of subsequent sessions, to try to reduce the number of authentication round trips. The server may accept these credentials if it considers them to be valid, or issue a new challenge to the client. This saved, or preferred, authentication mechanism can be read or written by the DM server via the AAuthPref node in the DMAcc object.

During the authentication phase, the DM client also accepts packages with only a challenge and no DM commands, as well as normal packages with both the challenge and some commands. Once authentication is done, however, an empty package signals the end of the session.

Server authentication in the client and client authentication to the server are two independent mechanisms. That is, any credentials sent from the client to the server in the first package is independent of which authentication mechanism the client requests from the server. For incoming challenges of the DM client from the server, the client responds with the corresponding credentials.

To authenticate the server, however, the client is configured to accept at least a "lowest acceptable authentication level" for the server credentials. When the client challenges the server, it tries to use the authentication level that the server used for its challenge in the last session, unless that was a less secure level than the "lowest acceptable authentication level". That is, the client always issues challenges to the server with an authentication level at least as secure as the "lowest acceptable" mechanism.

Example:

If the "lowest acceptable level" is configured to be MD5, the client never issues challenges with less secure mechanisms to the server or accepts, for example, Basic credentials from the server, but always challenges with at least MD5 level. Since the client and server authentications are completely independent, this restriction does not affect the preferred client credentials (AAuthPref). The DM client remembers the last incoming challenge and sends corresponding credentials in package 1, regardless of the security level. It also tries to use the same AAuthPref level to challenge the server, but with this restriction applied. That is, if AAuthPref is Basic the client sends its Basic credentials but a MD5 challenge to the server.

The HMAC authentication mechanism implies that the client accepts a new challenge for every package received from the server, in order to be given a new nonce to use with the next package. The client responds with Status = 200 for the SyncHdr and a new challenge to the server with the new nonce value for the server to use with the next package. In this way, all packages during the session contain a challenge to the counterpart to set NextNonce. Credentials are transferred in the HTTP headers of the packages. This behaviour is not standardised, but agreed upon through IOT discussions at, for instance, OMA TestFests. The DM client also accepts initial HMAC challenges from the server side, even though it is specified that the server must not be the first side to initiate HMAC authentication.

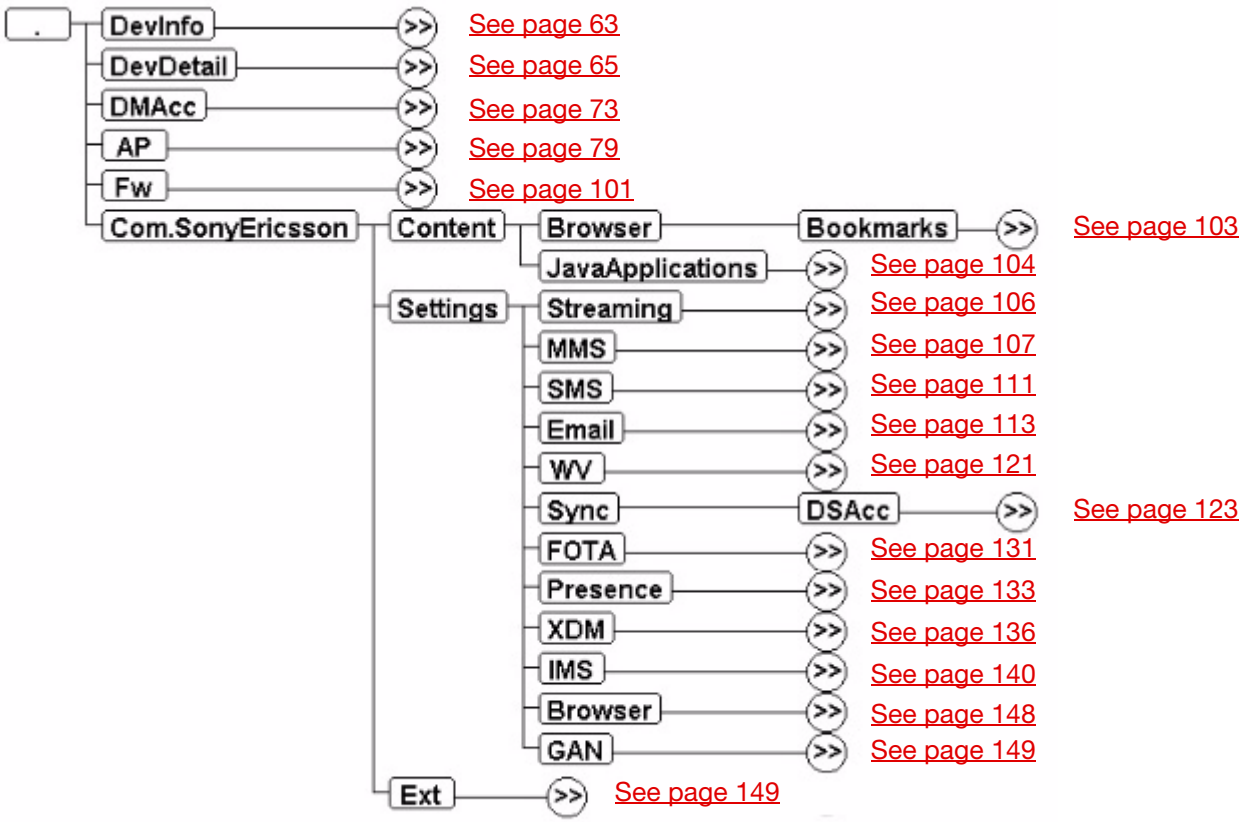
With mechanisms using nonce values, the client sends a challenge if the first credentials received from the server were wrong due to unsynchronised nonces. If the second answer from the server also contains errors, the authentication is regarded as having failed (since the server received a valid NextNonce in the client challenge) and the client disconnects even if the server package contains commands.

The client does not do any digest verification of package 0 (server notification package) and starts a session regardless of whether the digest is correct or not. In sessions started with a server notification, the client always requires server DM authentication even if package 0 did contain a valid digest. However, servers using a connection with transport security are always regarded as authenticated from start.

Management Objects

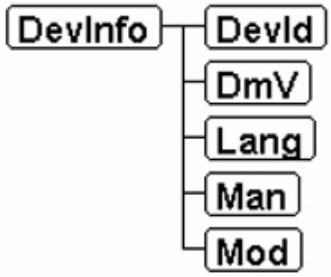
Basic tree structure for DM client versions 5.0 and 6.0

Note: The ./Com.SonyEricsson/Settings/WV and ./Com.SonyEricsson/Settings/IMS subtrees are **not supported** in DM version 6.



Device information subtree ./DevInfo

Subtree structure



./DevInfo

OMA standardised Management Object for device information.

Access Type: Get
Occurrence: One
Format: Node

./DevInfo/DevId

The IMEI number of the phone, formatted as a string, for example, `"IMEI:123456789012345"`.

Access Type: Get
Occurrence: One
Format: chr

./DevInfo/DmV

DM Client version. The value can be used to find the correct DDF published on the Sony Ericsson Web site.

Access Type: Get
Occurrence: One
Format: chr
Default Value: “`5.0`”

./DevInfo/Lang

Current language for the phone, for example, `"en"` for English.

Access Type: Get
Occurrence: One
Format: chr

./DevInfo/Man

Phone manufacturer.

Access Type: Get
Occurrence: One
Format: chr
Default Value: “SonyEricsson”

./DevInfo/Mod

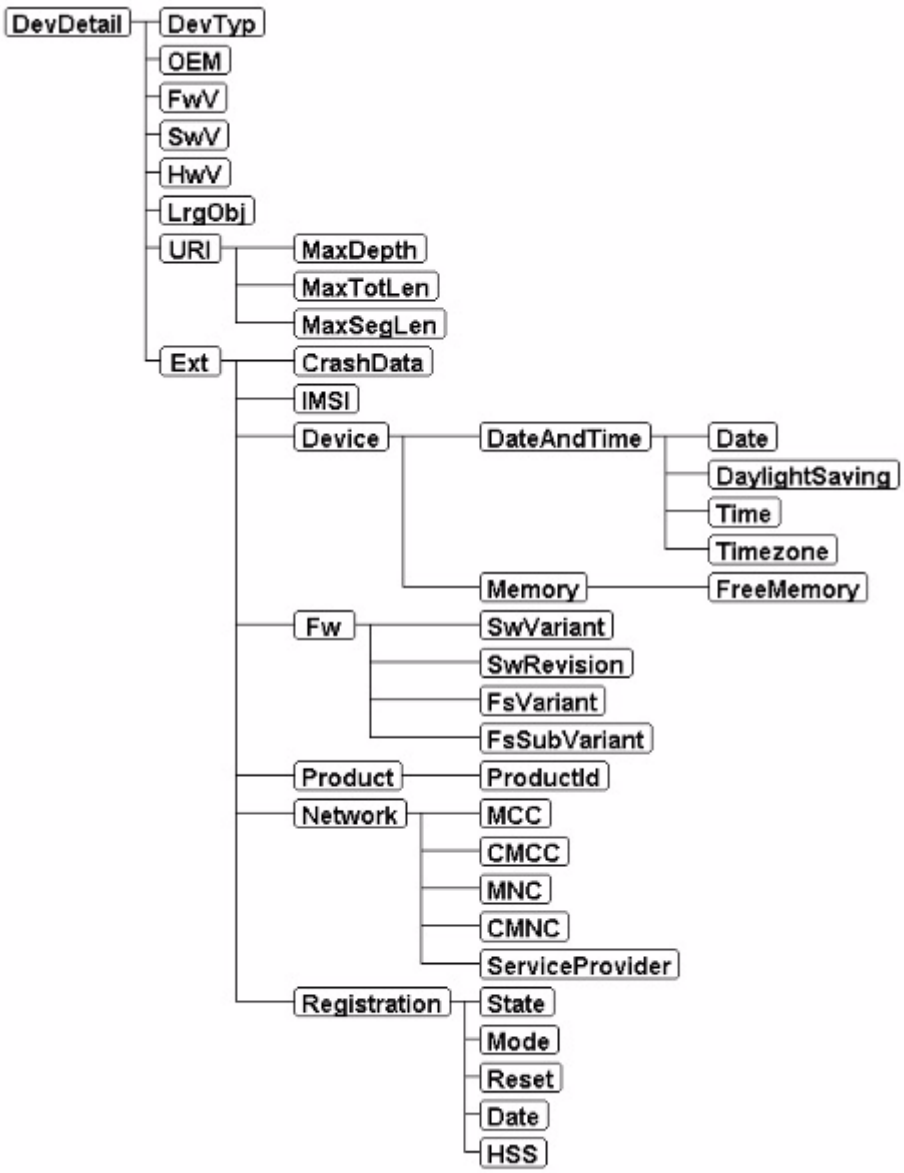
Phone model, for example, "C905"

Access Type: Get
Occurrence: One
Format: chr

Detailed device information ./DevDetail

OMA standardised object

Subtree structure



./DevDetail

OMA standardised Management Object for detailed device information (with Sony Ericsson specific extensions under the Ext internal node).

Access Type: Get
Occurrence: One
Format: Node

./DevDetail/DevTyp

Type of device.

Access Type: Get
Occurrence: One
Format: chr
Default Value: "phone"

./DevDetail/OEM

Original Equipment Manufacturer.

Access Type: Get
Occurrence: One
Format: chr
Default Value: "SonyEricsson"

./DevDetail/FwV

Concatenated Firmware Version identifier.

Access Type: Get
Occurrence: One
Format: chr

./DevDetail/SwV

Software version.

Access Type: Get
Occurrence: One
Format: chr

./DevDetail/HwV

Hardware version.

Access Type: Get
Occurrence: One
Format: chr

./DevDetail/LrgObj

Indicates whether the phone supports the SyncML Large Object Handling specification.

Access Type: Get
Occurrence: One
Format: bool
Default Value: True

./DevDetail/URI

Details about DM tree URI formatting.

Access Type: Get
Occurrence: One
Format: Node

./DevDetail/URI/MaxDepth

Specifies the maximum depth of the management tree supported by the phone. The maximum depth of the tree is defined as the maximum number of URI segments the phone supports. The value is a 16-bit, unsigned integer encoded as a numerical string. The value "0" means that the phone supports a tree of "unlimited" depth.

Access Type: Get
Occurrence: One
Format: chr
Default Value: "20"

./DevDetail/URI/MaxTotLen

Specifies the maximum total length of any URI used to address a node or node property. The maximum total length of a URI is defined as the largest total number of characters making up the URI the phone supports. Note that, depending on the character set, this might not be the same as the number of bytes. The value is a 16-bit, unsigned integer encoded as a numerical string. The value "0" means that the phone supports URI of "unlimited" length.

Access Type: Get
Occurrence: One
Format: chr
Default Value: "0"

./DevDetail/URI/MaxSegLen

Specifies the maximum total length of any URI segment in a URI used to address a node or node property. The maximum total length of a URI segment is defined as the largest number of characters the phone supports in a single URI segment. Note that, depending on the used character set, this might not be the same as the number of bytes. The value is a 16-bit, unsigned integer encoded as a numerical string. The value "0" means that the phone supports URI segments of "unlimited" length.

Access Type: Get
Occurrence: One
Format: chr
Default Value: "255"

./DevDetail/Ext

Sony Ericsson specific DevDetail extensions.

Access Type: Get
Occurrence: One
Format: Node

./DevDetail/Ext/CrashData

Binary representation of the Sony Ericsson crash data statistics object.

Access Type: Get
Occurrence: One
Format: bin

./DevDetail/Ext/IMSI

The IMSI formatted as an ASCII string of hexadecimal octets, for example, "`01 02 03 4A 5B FF`".

Access Type: Get
Occurrence: One
Format: chr

./DevDetail/Ext/Device

Settings and information about phone configuration.

Access Type: Get
Occurrence: One
Format: node

./DevDetail/Ext/Device/DateAndTime

Current date and time settings of the phone (read-only).

Access Type: Get
Occurrence: One
Format: node

./DevDetail/Ext/Device/DateAndTime/Date

Current date in the phone (GMT).

Access Type: Get
Occurrence: One
Format: chr
Allowed values: String, format “dd-mm-yyyy”

./DevDetail/Ext/Device/DateAndTime/DayLightSaving

Number of hours for daylight saving.

Access Type: Get
Occurrence: One
Format: int
Allowed values: Integer, in range `0` to `2`

./DevDetail/Ext/Device/DateAndTime/Time

Current time in the phone.

Access Type: Get
Occurrence: One
Format: chr
Allowed values: String, format “hh:mm”

./DevDetail/Ext/Device/DateAndTime/Timezone

Time zone offset relative to GMT.

Access Type: Get
Occurrence: One
Format: int
Allowed values: Integer, in range `-48` to `+51`. Time zone offset from GMT, specified in quarters of an hour

./DevDetail/Ext/Device/Memory

Memory status of the phone.

Access Type: Get
Occurrence: One
Format: node

./DevDetail/Ext/Device/Memory/FreeMemory

Amount of free space in the file system of the phone. Does not include space on the removable memory card.

Access Type: Get
Occurrence: One
Format: int

./DevDetail/Ext/Fw

Detailed firmware version information, for example, firmware update (FOTA) servers.

Access Type: Get
Occurrence: One
Format: Node

./DevDetail/Ext/Fw/SwVariant

Software CXC number.

Access Type: Get
Occurrence: One
Format: chr

./DevDetail/Ext/Fw/SwRevision
Software revision.

Access Type: Get
Occurrence: One
Format: chr

./DevDetail/Ext/Fw/FsVariant
File system version.

Access Type: Get
Occurrence: One
Format: chr

./DevDetail/Ext/Fw/FsSubVariant
File system area identifier.

Access Type: Get
Occurrence: One
Format: chr

./DevDetail/Ext/Product
Product-specific information.

Access Type: Get
Occurrence: One
Format: Node

./DevDetail/Ext/Product/ProductId
Identifier for customised product.

Access Type: Get
Occurrence: One
Format: chr

./DevDetail/Ext/Network
Network information.

Access Type: Get
Occurrence: One
Format: Node

./DevDetail/Ext/Network/MCC
Mobile Country Code.

Access Type: Get
Occurrence: One
Format: chr

./DevDetail/Ext/Network/CMCC

Current Mobile Country Code.

Access Type: Get
Occurrence: One
Format: chr

./DevDetail/Ext/Network/MNC

Mobile Network Code.

Access Type: Get
Occurrence: One
Format: chr

./DevDetail/Ext/Network/CMNC

Current Mobile Network Code.

Access Type: Get
Occurrence: One
Format: chr

./DevDetail/Ext/Network/ServiceProvider

Name of Service provider from SIM.

Access Type: Get
Occurrence: One
Format: chr

./DevDetail/Ext/Registration

Sony Ericsson Warranty Registration information.

Access Type: Get
Occurrence: One
Format: node

./DevDetail/Ext/Registration/State

Indicates the current mode of the registration date.

Access Type: Get
Occurrence: One
Format: chr
Allowed values:

Value	Description
“Client“	Date is relative to the phone clock
“NITZ”	Date is relative to a network time reference
“DM”	Date has been set via DM by a registration server

./DevDetail/Ext/Registration/Mode

Client registration mode.

Access Type: Get
Occurrence: One
Format: chr
Allowed values:

Value	Description
“None“	Not registered
“SMS”	Registration SMS sent
“DM”	Registered via a DM session

./DevDetail/Ext/Registration/Reset

Indicates if the real-time clock has been reset (when value is True).

Access Type: Get
Occurrence: One
Format: bool

./DevDetail/Ext/Registration/Date

The date when the phone was registered. Can only be written once.

Access Type: Get, Replace
Occurrence: One
Format: chr
Allowed values: String, format “dd-mm-yyyy”

./DevDetail/Ext/Registration/HSS

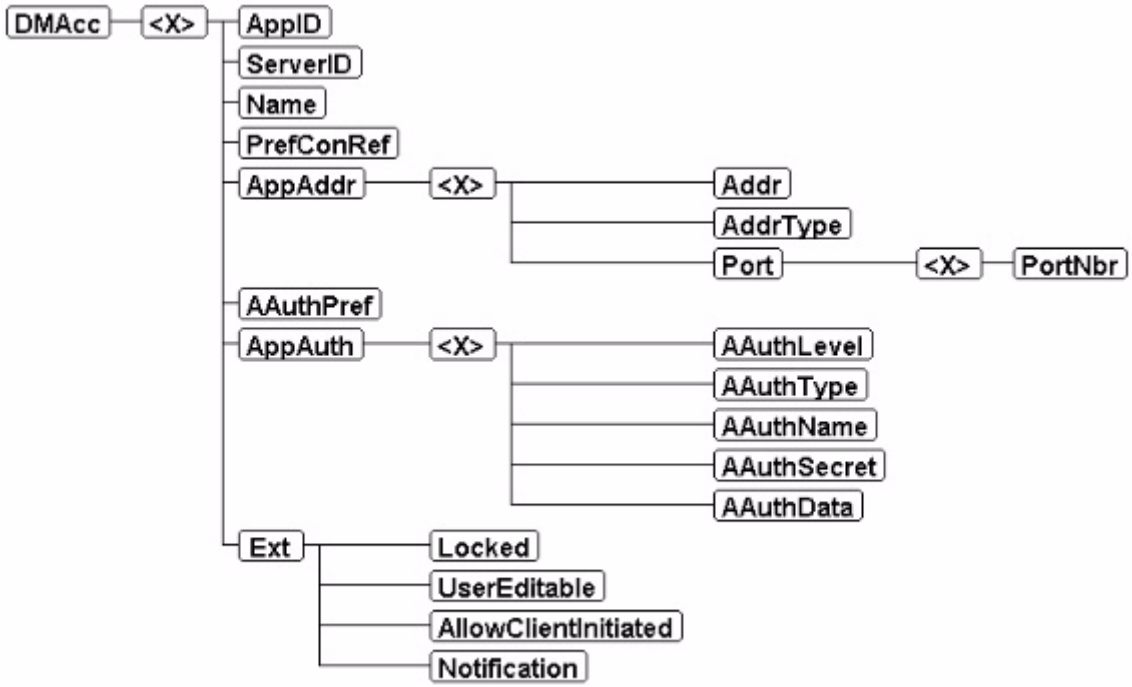
Hours Since Started.

Access Type: Get
Occurrence: One
Format: int
Allowed values: Integer, the number of hours since the client was started

DM accounts ver. 1.2

OMA standardised Management Object for DM 1.2 accounts.

Subtree structure



./DMAcc

OMA standardised Management Object for DM 1.2 accounts.

Access Type: Get
Occurrence: One
Format: Node

./DMAcc/X

This node is a placeholder representing one DM account.

Access Type: Add, Delete, Get
Occurrence: ZeroOrN (N<=5)
Format: Node

./DMAcc/X/AppID

This node specifies the application ID for one Device Management account object.

Access Type: Get
Occurrence: One
Format: chr
Default value: “w7“

./DMAcc/X/ServerID

This node specifies a server identifier for a management server used in the management session. The server ID cannot be replaced in an existing account. If it needs to be changed, the account has to be removed by deleting the placeholder and subsequently adding a new account with the new Server ID

Access Type: Add, Get
Occurrence: One
Format: chr
Allowed values: String, max length 79

./DMAcc/X/Name

This node specifies the user displayable name for the DM account.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 49

./DMAcc/X/PrefConRef

This node specifies a reference to the preferred data account object for connectivity, for example,
"./AP/AP-01".

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values:

Value	Description
"./AP/<X>"	<X> is the placeholder name for the linked account. The account must exist in the tree

./DMAcc/X/AppAddr

This node specifies management server addresses. The current implementation supports only one address.

Access Type: Add, Get
Occurrence: One
Format: Node

./DMAcc/X/AppAddr/X

This interior node acts as a placeholder, but currently only supports one server address.

Access Type: Add, Get
Occurrence: One
Format: Node

./DMAcc/X/AppAddr/X/Addr

This node specifies a management server address.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 255. Address format depends on AddrType, default is URI

./DMAcc/X/AppAddr/X/AddrType

This node specifies a management server address type.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Default Value: "URI"
Allowed values:

Value	Description
""	Use default value (that is, URI)
"URI"	Server address is an absolute URI
"IPv4"	
"IPv6"	

./DMAcc/X/AppAddr/X/Port

This node specifies port information for a management server address.

Access Type: Add, Get
Occurrence: ZeroOrOne
Format: Node

./DMAcc/X/AppAddr/X/Port/X

This interior node acts as a placeholder for separating one or more port settings. Current implementation only supports one port number.

Access Type: Add, Get
Occurrence: ZeroOrOne
Format: Node

./DMAcc/X/AppAddr/X/Port/X/PortNbr

This node specifies a port number.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr

./DMAcc/X/AAuthPref

This node indicates which authentication type to use when connecting to the server, that is, the last authentication type from the server challenge in an authenticated session.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Default value: "BASIC"
Allowed values:

Value	Description
""	Use default value, "syncml:auth-basic"
"BASIC"	DM "syncml:auth-basic" authentication
"DIGEST"	DM "syncml:auth-md5" authentication
"HMAC"	DM "syncml:auth-MAC" authentication

./DMAcc/X/AppAuth

This node specifies authentication information.

Access Type: Add, Get
Occurrence: ZeroOrOne
Format: Node

./DMAcc/X/AppAuth/X

This interior node acts as a placeholder to separate one or more authentication settings. The implementation currently supports a maximum of three unique settings: "CLCRED", "SRVCRED" and "HTTP". Only one setting is allowed for each type, for example, you cannot have two "CLCRED" placeholders.

Access Type: Add, Delete, Get
Occurrence: ZeroOrN (N<=3)
Format: Node

./DMAcc/X/AppAuth/X/AAuthLevel

This node specifies the authentication level. The value can only be specified by a server when the node is added, existing nodes are read-only.

Access Type: Add, Get
Occurrence: ZeroOrOne
Format: chr
Allowed values:

Value
"SRVCRED"
"CLCRED"
"HTTP"

./DMAcc/X/AppAuth/X/AAuthType

This node specifies the authentication type (read-only). This node has no meaning. All credentials in this subtree are used for all authentication types for the authentication level of the subtree.

Access Type: Get
Occurrence: ZeroOrOne
Format: chr

./DMAcc/X/AppAuth/X/AAuthName

This node specifies the authentication name.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 80

./DMAcc/X/AppAuth/X/AAuthSecret

This node specifies the authentication secret.

Access Type: Add, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 60

./DMAcc/X/AppAuth/X/AAuthData

This node specifies the authentication next nonce.

Access Type: Add, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 51.

./DMAcc/X/Ext

Sony Ericsson specific extensions.

Access Type: Add, Get
Occurrence: ZeroOrOne
Format: Node

./DMAcc/X/Ext/Locked

Indicates if this account is locked and cannot be edited or removed. A DM server can add the node with value True when adding a new account but cannot replace the value in existing accounts.

Access Type: Add, Get
Occurrence: ZeroOrOne
Format: bool
Defaultvalue: False

./DMAcc/X/Ext/UserEditable

Indicates if the user is allowed to edit this account via the UI.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: bool
Default value: True

./DMAcc/X/Ext/AllowClientInitiated

Indicates if this account can be used for a client-initiated session, that is, if the user can start a DM session via the UI.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: bool
Default value: True

./DMAcc/X/Ext/Notification

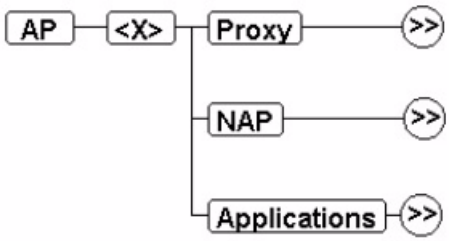
Determines how the user is notified of a server-initiated session request.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Default value: “ask”
Allowed values:

Value	Description
“ask“	The user is presented with a popup question to accept or reject the session
“accept”	No popup is presented to the user. The session is always accepted
“reject”	Server-initiated sessions are always rejected

Data accounts

Basic tree structure of the AP node



See page 80
See page 84
See page 99

./AP

Container for Access Point settings, that is, data accounts (NAP) and proxy settings (Proxy).

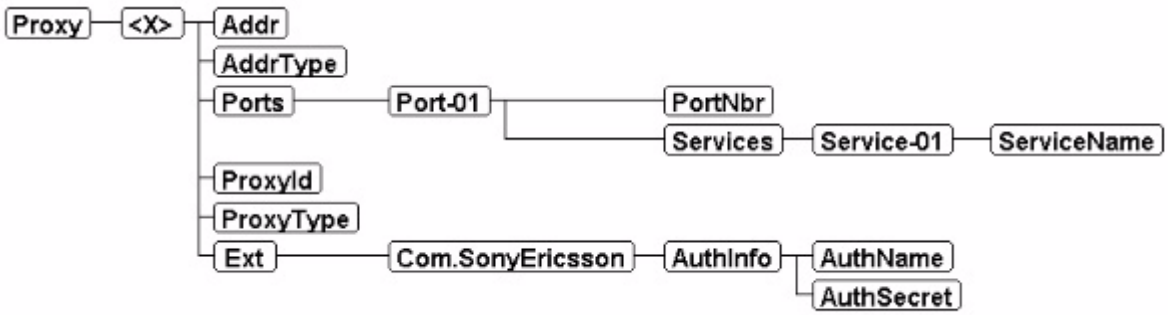
Access Type: Get
Occurrence: One
Format: Node

./AP/X

Name of an access point. Note that a NAP entry is required and BearerType must be set for this NAP entry to be valid. All AP entries without a valid NAP object will be discarded after the session if the client supports more than one bearer type.

Access Type: Add, Delete, Get
Occurrence: ZeroOrMore
Format: Node

./AP/X/Proxy subtree



./AP/X/Proxy

Root for proxy objects connected to the NAP object within the same AP subtree.

Access Type: Add, Get
Occurrence: One
Format: Node

./AP/X/Proxy/X

This interior node specifies the unique object ID of a proxy management object. The proxy is only used in connection with the NAP object within the same AP subtree. The number of proxies are limited to one for each type of protocol, that is, for each service. Three proxies can currently be defined within each AP object with the following services http (default), https and rtsp. If a default proxy cannot be set, a proxy without a valid service is discarded after the DM session has been completed.

Access Type: Add, Delete, Get
Occurrence: ZeroOrN (N <= 3)
Format: Node

./AP/X/Proxy/X/Addr

Proxy address.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 255, URL

./AP/X/Proxy/X/AddrType

This leaf node specifies the format of the Addr node. This node is required by the standard. It is set by the client to either IPv4 or ALPHA.

Access Type: Get
Occurrence: ZeroOrOne
Format: chr
Allowed values:

Value	Description
`"IPv4"`	An IPv4 address [AUTH-RFC791] represented in string form dotted-decimal CIDR notation (default)
`"ALPHA"`	Generic alphanumeric address as defined by alphanum in [AUTH-RFC2396-ALPHA]

./AP/X/Proxy/X/Ports

Access Type: Add, Get
Occurrence: One
Format: Node

./AP/X/Proxy/X/Ports/Port-01

Access Type: Add, Get
Occurrence: One
Format: Node

./AP/X/Proxy/X/Ports/Port-01/PortNbr

This leaf node defines the port number as a 16-bit unsigned integer, of a single port which is opened by this proxy.

Access Type: Add, Get, Replace
Occurrence: One
Format: Int
Allowed values: Integer in range 0 to 65535

./AP/X/Proxy//X/Ports/Port-01/Services

This interior node lists the services offered at the specified port.

Access Type: Add, Get
Occurrence: One
Format: Node

./AP/X/Proxy/X/Ports/Port-01/Services/Service-01

Access Type: Add, Get
Occurrence: One
Format: Node

./AP/X/Proxy/X/Ports/Port-01/Services/Service-01/ ServiceName

This leaf node identifies the name of a single service offered by a proxy.

Access Type: Add, Get
Occurrence: One
Format: chr
Default value: “`http`”
Allowed values:

Value	Description
`"http"`	The proxy is used for communication over http. (default)
`"https"`	Used for https traffic
`"rtsp"`	Used for streaming, using rtsp protocol

./AP/X/Proxy//X/ProxyId

This leaf node uniquely identifies this proxy Management Object. Identical to parent placeholder.

Access Type: Get
Occurrence: One
Format: chr

./AP/X/Proxy/X/ProxyType

The client currently supports proxies of type http as specified by OMA. The node always returns the value `"http"`.

Access Type: Get
Occurrence: ZeroOrOne
Format: chr
Default value: “`http`”

./AP/X/Proxy/X/Ext

Sony Ericsson specific extensions.

Access Type: Add, Get
Occurrence: One
Format: Node

./AP/X/Proxy/X/Ext/Com.SonyEricsson

Access Type: Add, Get
Occurrence: One
Format: Node

./AP/X/Proxy/X/Ext/Com.SonyEricsson/AuthInfo

Proxy authentication information.

Access Type: Add, Get
Occurrence: One
Format: Node

./AP/X/Proxy/X/Ext/Com.SonyEricsson/AuthInfo/AuthName

User credential used to authenticate the user.

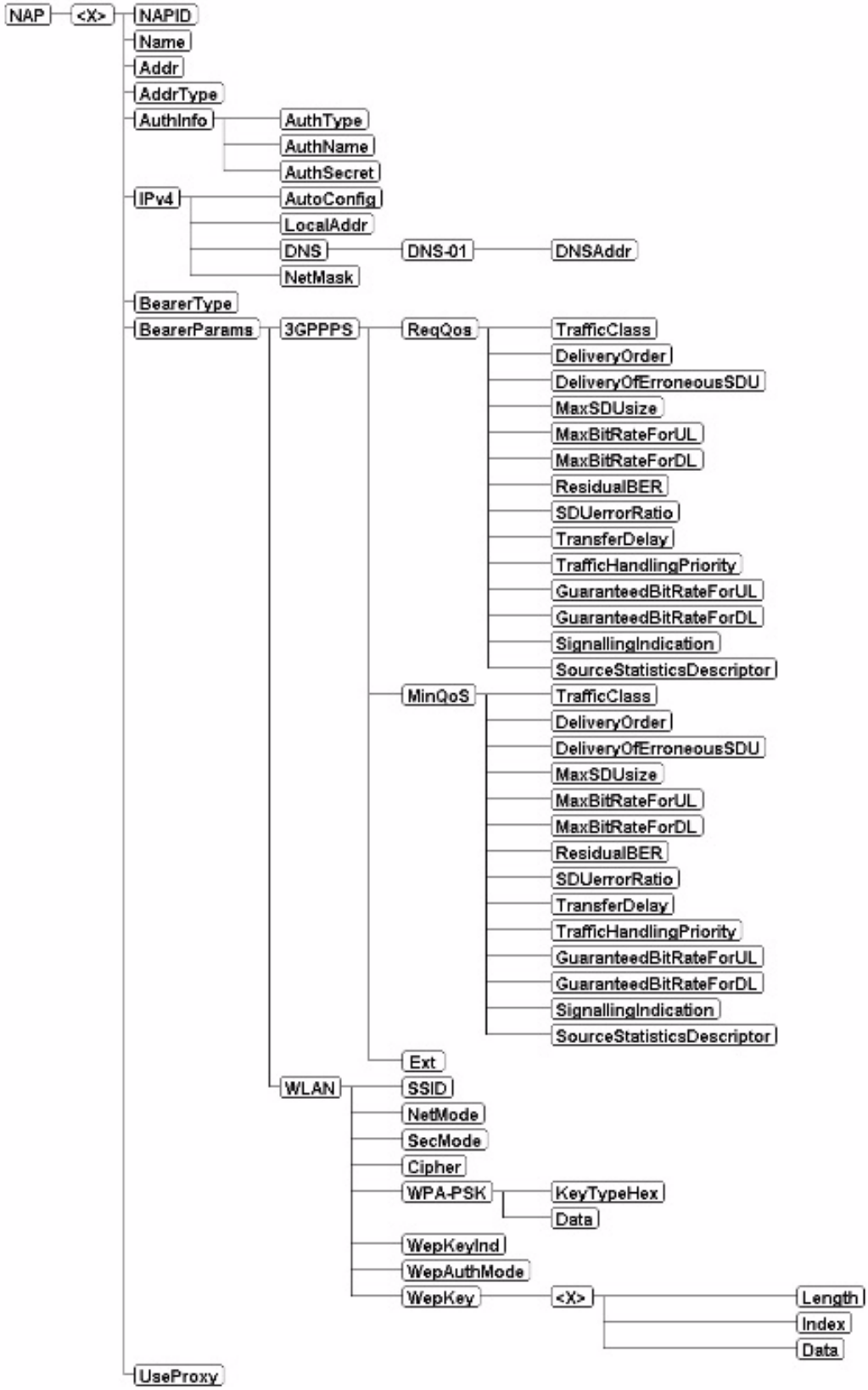
Access Type: Add, Get, Replace
Occurrence: One
Format: chr
Allowed values: String max length 80

./AP/X/Proxy/X/Ext/Com.SonyEricsson/AuthInfo/AuthSecret

Secret credential used to authenticate the user.

Access Type: Add, Replace
Occurrence: One
Format: chr
Allowed values: String max length 80

./AP/X/NAP subtree



./AP/X/NAP

Access Type: Add, Get
Occurrence: One
Format: Node

./AP/X/NAP/X

This interior node specifies the unique object ID of a Network Access Point (NAP) Management Object. Note that BearerType must be set for a NAP entry to be valid. For phone models supporting only one bearer type, this is set automatically at the end of the session. All AP subtrees with an undefined bearer type will be discarded after the session has ended.

Access Type: Add, Get
Occurrence: ZeroOrMore
Format: Node

./AP/X/NAP/X/NAPID

The device-assigned account ID. This node is read-only and automatically added by the DM client on existing accounts. It cannot be added by the DM server for new accounts.

Access Type: Get
Occurrence: One
Format: chr

./AP/X/NAP/X/Name

Displayable account name. The name is identical to the name of the parent placeholder.

Access Type: Get
Occurrence: ZeroOrOne
Format: chr

./AP/X/NAP/X/Addr

APN address. This parameter is **not** valid if Bearer Type is set to WLAN.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 99, URL

./AP/X/NAP/X/AddrType

This leaf node specifies the format of the **Addr** node. This node is required by the standard. It is set by the DM client to either "`IPv4`" or "`ALPHA`".

Access Type: Get
Occurrence: One
Format: chr
Allowed values:

Value	Description
"IPv4"	An IPv4 address [AUTH-RFC791] represented in string form dotted-decimal CIDR notation (default)
"ALPHA"	Generic alphanumeric address (as defined by alphanum in [AUTH-RFC2396-ALPHA])

./AP/X/NAP/X/AuthInfo

This interior node provides authentication credentials to support various forms of network access point authentication.

Access Type: Add, Get
Occurrence: One
Format: Node

./AP/X/NAP/X/AuthInfo/AuthType

Comma-separated list of any of the following authentication type strings. This parameter is **not** valid if Bearer Type is set to WLAN.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Default value: "None,PAP,CHAP"
Allowed values:

Value	Description
"None"	No authentication is needed
"Normal"	Alias for PAP
"Secure"	Alias for CHAP
"PAP"	Password Authentication Protocol
"CHAP"	Challenge Handshake Authentication Protocol
"MS CHAP"	Microsoft CHAP v1
"MS CHAP V2"	Microsoft CHAP v2

./AP/X/NAP/X/AuthInfo/AuthName

User name for authentication. This parameter is **not** valid if Bearer Type is set to WLAN.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 50

./AP/X/NAP/X/AuthInfo/AuthSecret

Authentication password. This parameter is **not** valid if Bearer Type is set to WLAN.

Access Type: Add, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String max length 50

./AP/X/NAP/X/IPv4

This interior node defines the IPv4 address configuration of the terminal.

Access Type: Add, Get
Occurrence: One
Format: Node

./AP/X/NAP/X/IPv4/AutoConfig

The terminal uses the IPv4 configuration specified in the LocalAddr parameter. Access Types Add and Replace when AutoConfig is set to False. However, if the LocalAddr parameter is configured statically, the AutoConfig parameter value automatically changes to False.

Access Type: Add, Get, Replace
Occurrence: ZeroOrMore
Format: bool
Default value: True

Value	Description
True	Dynamic IP configuration is used
False	Static IP configuration is used

./AP/X/NAP/X/IPv4/LocalAddr

This node specifies the IPv4 address. If configured statically, the AutoConfig value automatically changes to False.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Default value: “`0.0.0.0`”
Allowed values: IP number, "`0.0.0.0`" is Network Subscribe

./AP/X/NAP/X/IPv4/DNS

This node lists one DNS server address.

Access Type: Add, Get
Occurrence: One
Format: Node

./AP/X/NAP/X/IPv4/DNS/DNS-01

This node distinguishes DNS server addresses.

Access Type: Add, Get
Occurrence: One
Format: Node

./AP/X/NAP/X/IPv4/DNS/DNS-01/DNSAddr

DNS IP address.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Default value: “0.0.0.0”
Allowed values: IP number, "0.0.0.0" is Network Subscribe

./AP/X/NAP/X/IPv4/NetMask

This node specifies the IPv4 network address mask.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Default value: “0.0.0.0”
Allowed values: IP number

./AP/X/NAP/X/BearerType

This leaf node is used to define the bearer type used to reach this network access point. Note that all bearers are not supported by all phone models.

Access Type: Add, Get
Occurrence: ZeroOrOne
Format: chr
Default Value: “3GPPPS”
Allowed values:

Value	Description
"3GPPPS"	3GPP Packet Switched Bearer Parameters
"WLAN"	WLAN Parameter

./AP/X/NAP/X/BearerParams

Access Type: Add, Get
Occurrence: One
Format: Node

./AP/X/NAP/X/BearerParams/3GPPPS

This interior node specifies the 3GPP Packet Switched bearer specific Management Object for one Network Access Point (NAP) Management Object.

Access Type: Add, Get
Occurrence: One
Format: Node

./AP/X/NAP/X/BearerParams/3GPPPS/ReqQos

Requested Quality of Service.

Access Type: Add, Get
Occurrence: ZeroOrOne
Format: Node

./AP/X/NAP/X/BearerParams/3GPPPS/ReqQos/TrafficClass

Traffic class.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: 0
Allowed values: Integer in range 0 to 4

./AP/X/NAP/X/BearerParams/3GPPPS/ReqQos/DeliveryOrder

Delivery order.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: 0
Allowed values: Integer in range 0 to 2

./AP/X/NAP/X/BearerParams/3GPPPS/ReqQos/DeliveryOfErroneousSDU

Delivery of Erroneous SDU.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: 0
Allowed values: Integer in range 0 to 3

./AP/X/NAP/X/BearerParams/3GPPPS/ReqQos/MaxSDUsize

Maximum SDU size.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: `0`
Allowed values: Integer in range `0` to `153`

./AP/X/NAP/X/BearerParams/3GPPPS/ReqQos/MaxBitRateForUL

Maximum bit rate for uplink.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: `0`
Allowed values: Integer in range `0` to `255`

./AP/X/NAP/X/BearerParams/3GPPPS/ReqQos/MaxBitRateForDL

Maximum bit rate for downlink.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: `0`
Allowed values: Integer in range `0` to `255`

./AP/X/NAP/X/BearerParams/3GPPPS/ReqQos/ResidualBER

Residual BER.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: `7`
Allowed values: Integer in range `0` to `9`

./AP/X/NAP/X/BearerParams/3GPPPS/ReqQos/SDUerrorRatio

SDU error ratio.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: `4`
Allowed values: Integer in range `0` to `7`

./AP/X/NAP/X/BearerParams/3GPPPS/ReqQos/TransferDelay

Transfer delay.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: `0`
Allowed values: Integer in range `0` to `62`

./AP/X/NAP/X/BearerParams/3GPPPS/ReqQos/TrafficHandlingPriority

Traffic handling priority.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: `0`
Allowed values: Integer in range `0` to `3`

./AP/X/NAP/X/BearerParams/3GPPPS/ReqQos/GuaranteedBitRateForUL

Guaranteed bit rate for uplink.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: `0`
Allowed values: Integer in range `0` to `255`

./AP/X/NAP/X/BearerParams/3GPPPS/ReqQos/GuaranteedBitRateForDL

Guaranteed bit rate for downlink.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: `0`
Allowed values: Integer in range `0` to `255`

./AP/X/NAP/X/BearerParams/3GPPPS/ReqQos/SignallingIndication

Signalling indication.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: `0`
Allowed values: Integer in range `0` to `1`

./AP/X/NAP/X/BearerParams/3GPPPS/ReqQos/SourceStatisticsDescriptor

Source statistics descriptor.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: `0`
Allowed values: Integer in range `0` to `1`

./AP/X/NAP/X/BearerParams/3GPPPS/MinQos

Minimum Quality of service.

Access Type: Add, Get
Occurrence: ZeroOrOne
Format: Node

./AP/X/NAP/X/BearerParams/3GPPPS/MinQos/TrafficClass

Traffic class.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: `4`
Allowed values: Integer in range `1` to `4`

./AP/X/NAP/X/BearerParams/3GPPPS/MinQos/DeliveryOrder

Delivery order.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: `2`
Allowed values: Integer in range `1` to `2`

./AP/X/NAP/X/BearerParams/3GPPPS/MinQos/DeliveryOfErroneousSDU

Delivery of erroneous SDU.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: `3`
Allowed values: Integer in range `1` to `3`

./AP/X/NAP/X/BearerParams/3GPPPS/MinQos/MaxSDUsize

Maximum SDU size.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: `0`
Allowed values: Integer in range `0` to `153`

./AP/X/NAP/X/BearerParams/3GPPPS/MinQos/MaxBitRateForUL

Maximum bit rate for uplink.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: `0`
Allowed values: Integer in range `0` to `255`

./AP/X/NAP/X/BearerParams/3GPPPS/MinQos/MaxBitRateForDL

Maximum bit rate for downlink.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: `0`
Allowed values: Integer in range `0` to `255`

./AP/X/NAP/X/BearerParams/3GPPPS/MinQos/ResidualBER

Residual BER.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: `0`
Allowed values: Integer in range `0` to `9`

./AP/X/NAP/X/BearerParams/3GPPPS/MinQos/SDUerrorRatio

SDU error ratio.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: `0`
Allowed values: Integer in range `0` to `7`

./AP/X/NAP/X/BearerParams/3GPPPS/MinQos/TransferDelay

Transfer delay.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: `0`
Allowed values: Integer in range `0` to `62`

./AP/X/NAP/X/BearerParams/3GPPPS/MinQos/TrafficHandlingPriority

Traffic handling priority.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: `0`
Allowed values: Integer in range `0` to `3`

./AP/X/NAP/X/BearerParams/3GPPPS/MinQos/GuaranteedBitRateForUL

Guaranteed bit rate for uplink.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: `0`
Allowed values: Integer in range `0` to `255`

./AP/X/NAP/X/BearerParams/3GPPPS/MinQos/GuaranteedBitRateForDL

Guaranteed bit rate for downlink.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: `0`
Allowed values: Integer in range `0` to `255`

./AP/X/NAP/X/BearerParams/3GPPPS/MinQos/SignallingIndication

Signalling indication.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: `0`
Allowed values: Integer in range `0` to `1`

./AP/X/NAP/X/BearerParams/3GPPPS/MinQos/SourceStatisticsDescriptor

Source statistics descriptor.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default value: `0`
Allowed values: Integer, range `0` to `1`

./AP/X/NAP/X/BearerParams/3GPPPS/Ext

Sony Ericsson specific extensions.

Access Type: Add, Get
Occurrence: ZeroOrOne
Format: Node

./AP/X/NAP/X/BearerParams/WLAN

This interior node specifies the bearer specific parameters for a Network Access Point (NAP) Management Object describing a WLAN access point. The parameters below this node are not valid if BearerType is set to 3GPPPS.

Access Type: Add, Get
Occurrence: One
Format: Node

./AP/X/NAP/X/BearerParams/WLAN/SSID

The SSID parameter indicates the primary SSID (name) of the WLAN network.

Access Type: Add, Get, Replace
Occurrence: One
Format: chr
Default value: `"DEFAULT"`

./AP/X/NAP/X/BearerParams/WLAN/NetMode

The NetMode parameter indicates the operational mode of the WLAN. If the parameter is not set or if the parameter is omitted, then infrastructure mode is assumed.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Default value: `INFRA`
Allowed values:

Value	Description
`"INFRA"`	Infrastructure network
`"ADHOC"`	Ad hoc network

./AP/X/NAP/X/BearerParams/WLAN/SecMode

The SecMode parameter indicates the security mode for the WLAN network. If the parameter is omitted, no security is applied. If no meaningful combination of Cipher parameter value and SecMode parameter value is set, the SecMode parameter is set to "UNKNOWN".

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values:

Value	Description
"WEP"	WEP security in use
"WPA"	Wi-Fi Protected Access security in use
"WPA-PSK"	Wi-Fi Protected Access security using pre-shared key in use
"WPA2"	Wi-Fi Protected Access 2 security in use
"WPA2-PSK"	Wi-Fi Protected Acess 2 security using pre-shared key in use

./AP/X/NAP/X/BearerParams/WLAN/Cipher

The Cipher parameter specifies the encryption cipher to be used with this network access point. If the parameter is omitted or its value is null, no encryption is applied.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values:

	Description
null	No encryption
"WEP"	WEP encryption in use
"TKIP"	Temporary Key Integrity Protocol (TKIP) encryption
"AES"	Advanced Encryption Standard (AES) encryption

./AP/X/NAP/X/BearerParams/WLAN/WPA-PSK

This interior node groups together the parameters of WPA-PSK.
Note: This node and its subtree are meaningful only if SecMode value is WPA-PSK or WPA2-PSK.

Access Type: Add, Get
Occurrence: ZeroOrOne
Format: Node

./AP/X/NAP/X/BearerParams/WLAN/WPA-PSK/KeyTypeHex

The parameter indicates whether the following WPA-PSK data is provided as an ASCII string or as a hexadecimal digit sequence.

Access Type: Get
Occurrence: ZeroOrOne
Format: bool
Allowed values:

Value	Description
False	The WPA-PSK data is an ASCII string
True	The WPA-PSK data is a hexadecimal digit sequence

./AP/X/NAP/X/BearerParams/WLAN/WPA-PSK/Data

The parameter is used to deliver the WPA-PSK data. If the KeyTypeHex value is False, the Data parameter value is an ASCII string, 8 to 63 characters. If the KeyTypeHex value is True, the Data parameter value is a hexadecimal key, 64 hex characters.

Access Type: Add, Get, Replace
Occurrence: One
Format: chr

./AP/X/NAP/X/BearerParams/WLAN/WepKeyInd

The WepKeyInd parameter indicates the value of the Index node in the WepKey subtree representing the default WEP key.
Note: The keys specified in the WepKey subtree and the value of WepKeyInd are meaningful only if SecMode value is WEP.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Allowed values: integer, range 0 to 3

./AP/X/NAP/X/BearerParams/WLAN/WepAuthMode

The WepAuthMode parameter indicates WEP authentication mode.
Note: This node is meaningful only if SecMode value is WEP.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Default value: “OPEN”
Allowed values:

Value	Description
"OPEN"	Open Authentication Mode is used
"SHARED"	Shared Authentication Mode is used

./AP/X/NAP/X/BearerParams/WLAN/WepKey

This interior node defines the length and the data for the WEP key. The maximum number of keys is 4. The client **must** use the key with an Index value matching the value of the WepKeyInd node (if that node is included).

Access Type: Add, Get
Occurrence: ZeroOrOne
Format: Node

./AP/X/NAP/X/BearerParams/WLAN/WepKey/X

This interior node distinguishes different WEP keys. There can be up to four interior nodes on this level.

Access Type: Add, Get
Occurrence: ZeroOrN (N<=4)
Format: Node

./AP/X/NAP/X/BearerParams/WLAN/WepKey/X/Length

This parameter specifies the length of the WEP key in bytes.

Access Type: Get
Occurrence: One
Format: int
Allowed values: Integer, 5 or 13

./AP/X/NAP/X/BearerParams/WLAN/WepKey/X/Index

This parameter specifies the index of this WEP key as an integer value between 0 and 3. The first key is saved as index 0, the second as index 1, and so on.

Access Type: Get
Occurrence: One
Format: int
Allowed values: Integer, 0 to 3

./AP/X/NAP/X/BearerParams/WLAN/WepKey/X/Data

The Data parameter indicates the WEP key. WEP keys are either 5 bytes or 13 bytes long. The key is an ASCII string of hexadecimal digits where every digit is represented by one byte.

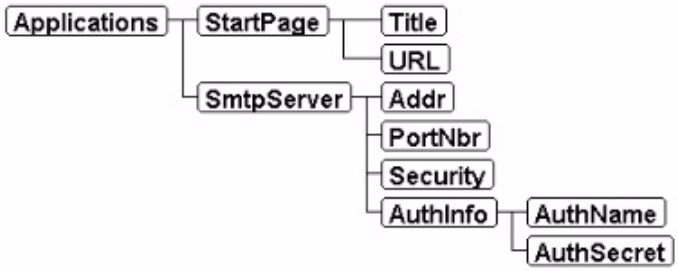
Access Type: Add, Get, Replace
Occurrence: One
Format: chr

./AP/X/NAP/X/UseProxy

Enable/disable proxies for the corresponding AP. Proxy data has to be defined for this AP for this value to be handled.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: bool
Default value: True

./AP/X/Applications subtree



./AP/X/Applications

Root for application specific settings used in combination with the NAP object within the same AP subtree.

Access Type: Add, Get
Occurrence: One
Format: Node

./AP/X/Applications/StartPage

Default browser start page when browsing using this AP.

Access Type: Add, Get
Occurrence: One
Format: Node

./AP/X/Applications/StartPage/Title

Displayable title for the start page.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 196

./AP/X/Applications/StartPage/URL

URL for start page.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 1024, URL

./AP/X/Applications/SmtpServer

SMTP server settings used when sending email using this AP.

Access Type: Add, Get
Occurrence: One
Format: Node

./AP/X/Applications/SmtpServer/Addr

SMTP server address.

Access Type: Add, Get, Replace
Occurrence: One
Format: chr
Allowed values: String, max length 31

./AP/X/Applications/SmtpServer/PortNbr

Port number.

Access Type: Add, Get, Replace
Occurrence: One
Format: int
Default value: `0`
Allowed values: Integer in range `0` to `65535`

./AP/X/Applications/SmtpServer/Security

Used security method.

Access Type: Add, Get, Replace
Occurrence: One
Format: chr
Default value: “`None`”
Allowed values:

Value	Description
`"None"`	
`"SSL"`	Secure connection over specified port
`"TLS"`	Secure MAP over TLS

./AP/X/Applications/SmtpServer/AuthInfo

Container for authentication information used when connecting to the server.

Access Type: Add, Get
Occurrence: One
Format: Node

./AP/X/Applications/SmtpServer/AuthInfo/AuthName

SMTP User name.

Access Type: Add, Get, Replace
Occurrence: One
Format: chr
Allowed values: String, max length 80

./AP/X/Applications/SmtpServer/AuthInfo/AuthSecret

SMTP User password.

Access Type: Add, Replace
Occurrence: One
Format: chr
Allowed values: String, max length 40

FUMO

OMA standardised object

Subtree structure

./Fw

OMA standardised Management Object for FUMO (Firmware Update over-the-air Management Object).

Access Type: Get
Occurrence: One
Format: Node

./Fw/FwPkg01

Firmware update package information.

Access Type: Get
Occurrence: One
Format: Node

./Fw/FwPkg01/State

Contains a value indicating the current state of the phone with respect to this firmware update. For a table of allowed values and their meaning, see the OMA FUMO documentation.

Access Type: Get
Occurrence: One
Format: int

./Fw/FwPkg01/Download

This interior node is the target of an `Exec` command invoked to initiate a firmware download for the specified update package.

Access Type: Exec, Get
Occurrence: One
Format: Node

./Fw/FwPkg01/Download/PkgURL

This node specifies the URL where the firmware update package or download descriptor is located.

Access Type: Get, Replace
Occurrence: One
Format: chr

./Fw/FwPkg01/Update

This interior node is a target of an `Exec` command invoked to initiate a firmware update for the specified update package.

Access Type: Exec, Get
Occurrence: One
Format: Node

./Fw/FwPkg01/Update/PkgData

This node is the target of a `Replace` command when DM is used to provide the binary firmware update package.

Access Type: Replace
Occurrence: One
Format: bin

./Fw/FwPkg01/DownloadAndUpdate

This interior node is the target of an `Exec` command invoked to initiate a firmware download and an immediate update for the specified update package.

Access Type: Exec, Get
Occurrence: One
Format: Node

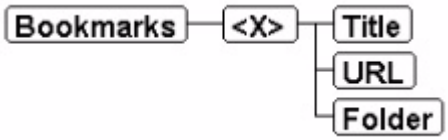
./Fw/FwPkg01/DownloadAndUpdate/PkgURL

This node specifies the URL where the firmware update package, that is to be downloaded and immediately installed, or its download descriptor is located.

Access Type: Get, Replace
Occurrence: One
Format: chr

Browser bookmarks

Subtree structure



./Com.SonyEricsson/Content/Browser/Bookmarks

Container for bookmark objects.

Access Type: Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Content/Browser/Bookmarks/X

A placeholder for bookmark settings. A new bookmark can be added to the browser list by adding a placeholder and at least the Title and URL leaf nodes.

Access Type: Get, Add, Delete
Occurrence: ZeroOrMore
Format: Node

./Com.SonyEricsson/Content/Browser/Bookmarks/X/Title

Displayable title of the bookmark.

Access Type: Get, Add, Replace
Occurrence: One
Format: chr
Values: String, max length 15

./Com.SonyEricsson/Content/Browser/Bookmarks/X/URL

Bookmark URL.

Access Type: Get, Add, Replace
Occurrence: One
Format: chr
Values: String, max length 512

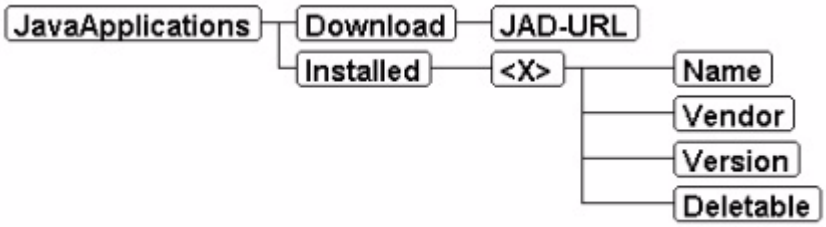
./Com.SonyEricsson/Content/Browser/Bookmarks/X/Folder

Folder in which the bookmark is grouped.

Access Type: Get, Add, Replace
Occurrence: ZeroOrOne
Format: chr

Third-party Java™ application download/ installation

Subtree structure



./Com.SonyEricsson/Content/JavaApplications

This is a management object that allows listing, deleting and triggering of external download/installation of third party Java™ applications.

Access Type: Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Content/JavaApplications/Download

Used for downloading and installation of new third-party Java applications. The download mechanism works in much the same way as downloads of FOTA packets via OMA download. First a URL to a JAD or JAR file in the child node JAD-URL is specified, then an Execute command is performed on this node. The download starts directly after the current DM session has ended.

Currently, the only way of knowing if the download and installation were successful, is to look for the new application among the ones listed under “Installed” in a subsequent DM session.

If more than one Execute command is sent during the same session, only the first is successful but the pending download operation still starts when the DM session has ended.

Access Type: Exec, Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Content/JavaApplications/Download/ JAD-URL

URL to the JAD or JAR file to download. If a URL is not specified prior to an Exec command on the Download node, the Execute command fails.

Access Type: Get, Replace
Occurrence: One
Format: chr
Allowed values: String, URL

./Com.SonyEricsson/Content/JavaApplications/Installed

This node contains a list of the applications currently installed in the phone. New placeholders cannot be added, the only way to install new applications is to use the Download/JAD-URL mechanism. Applications flagged as “deletable” can be deleted by performing a Delete command on the corresponding placeholder.

Access Type: Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Content/JavaApplications/Installed/X

A placeholder for installed applications. The default naming convention lists applications in the form "`JavaApp-XX`" where XX is a running number starting with 01.

Access Type: Delete, Get, Replace
Occurrence: ZeroOrMore
Format: Node

./Com.SonyEricsson/Content/JavaApplications/Installed/X/Name

The name of the application.

Access Type: Get
Occurrence: One
Format: chr

./Com.SonyEricsson/Content/JavaApplications/Installed/X/Vendor

The vendor string of the application.

Access Type: Get
Occurrence: One
Format: chr

./Com.SonyEricsson/Content/JavaApplications/Installed/X/Version

Version information for the application.

Access Type: Get
Occurrence: One
Format: chr

./Com.SonyEricsson/Content/JavaApplications/Installed/X/Deletable

Flag that indicates if the application can be removed or not. Note that deletable applications are removed without any user confirmation or even notification, so this flag should be used with care.

Access Type: Get
Occurrence: One
Format: bool

Streaming settings

Subtree structure

./Com.SonyEricsson/Settings/Streaming

Settings for media content streaming.

Access Type: Get
Occurrence: One
Format: Node

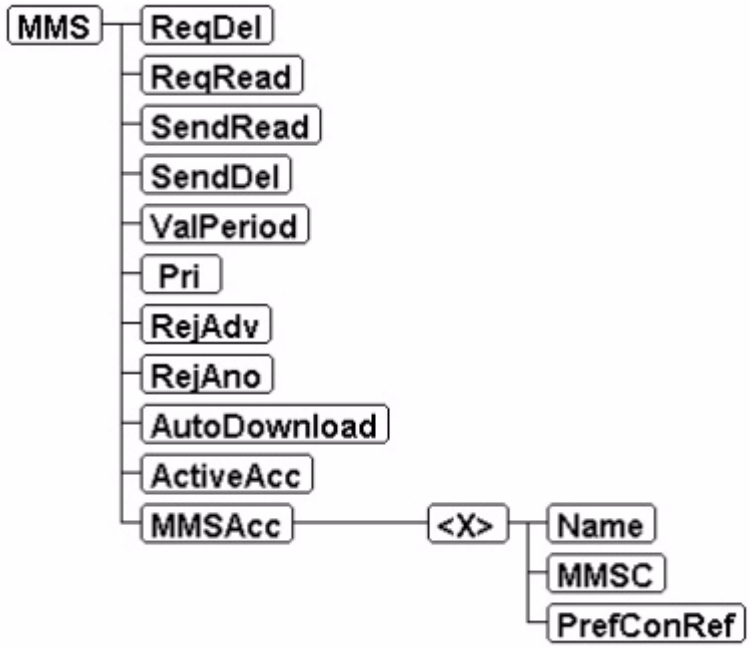
./Com.SonyEricsson/Settings/Streaming/PrefConRef

This node specifies a reference to preferred data account object for connectivity, for example,
"`./AP/AP-01`".

Access Type: Get, Replace
Occurrence: One
Format: chr
Allowed value: "`./AP/X`", where X is the placeholder name for the linked account. The account must exist in the tree.

MMS application settings

Subtree structure



./Com.SonyEricsson/Settings/MMS

Settings for the MMS (picture messaging) application.

Access Type: Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Settings/MMS/ReqDel

Request delivery report.

Access Type: Get, Replace
Occurrence: One
Format: bool
Default value: False

./Com.SonyEricsson/Settings/MMS/ReqRead

Request read report.

Access Type: Get, Replace
Occurrence: One
Format: bool
Default value: False

./Com.SonyEricsson/Settings/MMS/SendRead

Send read report.

Access Type: Get, Replace
Occurrence: One
Format: chr
Default value: “Conf”
Allowed values:

Value	Description
"On"	
"Off"	
"Conf"	Lets the user confirm

./Com.SonyEricsson/Settings/MMS/SendDel

Send delivery report.

Access Type: Get, Replace
Occurrence: One
Format: bool
Default value: True

./Com.SonyEricsson/Settings/MMS/ValPeriod

Validity period.

Access Type: Get, Replace
Occurrence: One
Format: chr
Default value: “Maximum”
Allowed values:

Value	Description
“1h”	One hour
“12h”	12 hours
“1day”	24 hours
“1week”	One week
“Maximum”	Network maximum

./Com.SonyEricsson/Settings/MMS/Pri

Message priority.

Access Type: Get, Replace
Occurrence: One
Format: chr
Default value: “Normal”
Allowed values: “Low”, “Normal”, “High”, “Unknown”

./Com.SonyEricsson/Settings/MMS/RejAdv

Reject advertisement.

Access Type: Get, Replace
Occurrence: One
Format: bool
Default value: False

./Com.SonyEricsson/Settings/MMS/RejAno

Reject anonymous.

Access Type: Get, Replace
Occurrence: One
Format: bool
Default value: False

./Com.SonyEricsson/Settings/MMS/AutoDownload

Determines under which circumstances Auto download is allowed.

Access Type: Get, Replace
Occurrence: One
Format: chr
Default value: “Always”
Allowed values: “Always”, “AskInRoaming”, “NeverInRoaming”, “Ask”, “Never”

./Com.SonyEricsson/Settings/MMS/ActiveAcc

Path to the currently active MMS profile placeholder in the DM tree, for example, “./Com.SonyEricsson/Settings/MMS/MMSProfile/MMSProfile-01", if a profile named "MMSProfile-01" exists.

Access Type: Get, Replace
Occurrence: One
Format: chr
Allowed values: "./Com.SonyEricsson/Settings/MMS/MMSProfile/<X>", where <X> is the placeholder name for the linked account. This account must exist in the tree.

./Com.SonyEricsson/Settings/MMS/MMSAcc

Container for a number of possible MMS accounts.

Access Type: Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Settings/MMS/MMSAcc/X

This node acts as a placeholder for a MMS account.

Access Type: Add, Delete, Get
Occurrence: ZeroOrN (N<=10)
Format: Node

./Com.SonyEricsson/Settings/MMS/MMSAcc/X/Name

Displayable name for this account.

Access Type: Add, Get, Replace
Occurrence: One
Format: chr
Allowed values: String, max length 16

./Com.SonyEricsson/Settings/MMS/MMSAcc/X/MMSC

Message server address.

Access Type: Add, Get, Replace
Occurrence: One
Format: chr
Allowed values: String, max length 50, Values are defined in 3GPP TS 23.140

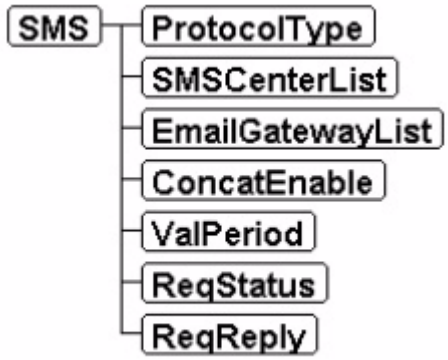
./Com.SonyEricsson/Settings/MMSAcc/X/PrefConRef

This node specifies a reference to preferred data account object for connectivity, for example,
"`./AP/AP-01`".

Access Type: Add, Get, Replace
Occurrence: One
Format: chr
Allowed values: "`./AP/<X>`", where <X> is the placeholder name for the linked account. This account must exist in the tree.

SMS settings

Subtree structure



./Com.SonyEricsson/Settings/SMS

Settings for the SMS (text messaging) application.

Access Type: Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Settings/SMS/ProtocolType

Protocol type.

Access Type: Get, Replace
Occurrence: One
Format: chr
Default Value: “Text”
Allowed values: “Text”, “Email”, “FaxGroup3”, “FaxGroup4”, “Voice”, “ERMES”, “Pager”

./Com.SonyEricsson/Settings/SMS/SMSCenterList

A comma-separated list of SMS service centre addresses (phone numbers). Usually a maximum of 5 numbers (depending on the limits of the SIM in use) of maximum 20 characters each, including optional leading "+". Valid characters are "0"-"9", "*" and "#". Example: "+4640107107,1234,8*4#21".

Note: If more than the maximum numbers are replaced, the DM client indicates this error with a status of 400, but the first correct numbers are accepted. In this way, a subsequent Get on the node returns the (typically) 5 first numbers of the failed replace.

Access Type: Get, Replace
Occurrence: One
Format: chr

./Com.SonyEricsson/Settings/SMS/EmailGatewayList

A comma-separated list of SMS Email Gateway addresses (phone numbers). Usually a maximum of 5 numbers (depending on the limits of the SIM in use) of maximum 20 characters each, including optional leading "+". Valid characters are "0"-"9", "*" and "#". Example: `"+4640107107,1234,8*4#21"`.

Note: If more than the maximum numbers are replaced, the DM client indicates this error with a status of 400, but the first correct numbers are accepted. In this way, a subsequent Get on the node returns the (typically) 5 first numbers of the failed replace.

Access Type: Get, Replace
Occurrence: One
Format: chr

./Com.SonyEricsson/Settings/SMS/ConcatEnable

Allows concatenated messages.

Access Type: Get, Replace
Occurrence: One
Format: bool
Default Value: True

./Com.SonyEricsson/Settings/SMS/ValPeriod

Validity period.

Access Type: Get, Replace
Occurrence: One
Format: chr
Default Value: “`Maximum`”
Allowed values:

Value	Description
“1h”	One hour
“12h”	12 hours
“1day”	24 hours
“1week”	One week
“Maximum”	Network maximum

./Com.SonyEricsson/Settings/SMS/ReqStatus

Request delivery status report.

Access Type: Get, Replace
Occurrence: One
Format: bool
Default Value: False

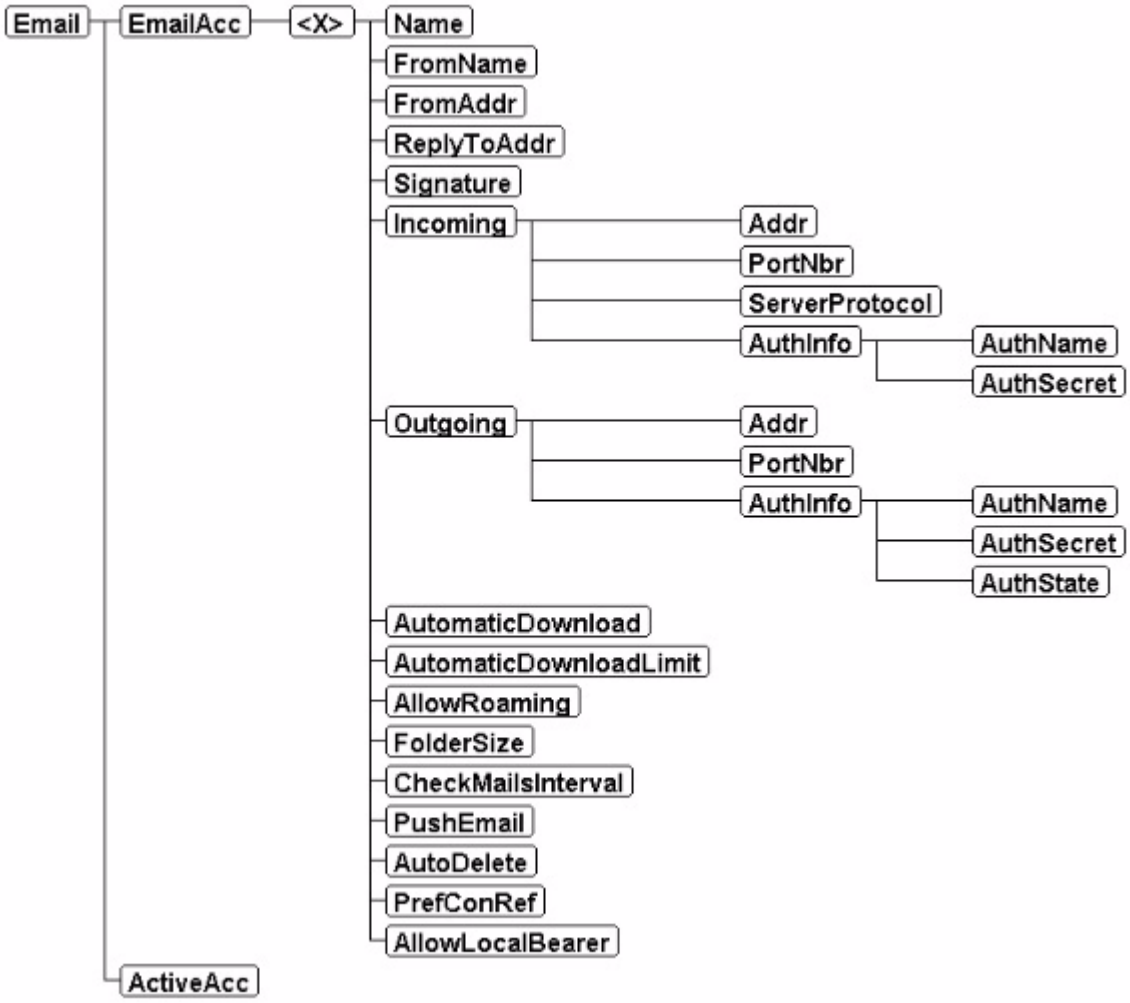
./Com.SonyEricsson/Settings/SMS/ReqReply

Request reply.

Access Type: Get, Replace
Occurrence: One
Format: bool
Default Value: False

Email accounts

Subtree structure



./Com.SonyEricsson/Settings/Email

Settings for the email application.

Access Type: Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Settings/Email/EmailAcc

Access Type: Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Settings/Email/EmailAcc/X

Placeholder representing an email account.

Access Type: Add, Delete, Get
Occurrence: ZeroOrN (N<=10)
Format: Node

./Com.SonyEricsson/Settings/Email/EmailAcc/X/Name

Displayable name for the email account.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 20

./Com.SonyEricsson/Settings/Email/EmailAcc/X/FromName

Full name of the user, added to outgoing mail.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 80

./Com.SonyEricsson/Settings/Email/EmailAcc/X/FromAddr

Email address.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 80

./Com.SonyEricsson/Settings/Email/EmailAcc/X/ReplyToAddr

An optional email address to which direct replies are sent.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 80

./Com.SonyEricsson/Settings/Email/EmailAcc/X/Signature

Signature.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 200

./Com.SonyEricsson/Settings/Email/EmailAcc/X/Incoming

Settings for incoming mail.

Access Type: Add, Get
Occurrence: ZeroOrOne
Format: Node

./Com.SonyEricsson/Settings/Email/EmailAcc/X/Incoming/Addr

Incoming server address.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 31

./Com.SonyEricsson/Settings/Email/EmailAcc/X/Incoming/PortNbr

Port number.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default Value: 110
Allowed values: Integer in range 0 to 65535

./Com.SonyEricsson/Settings/Email/EmailAcc/X/Incoming/ServerProtocol

Incoming server protocol.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Default Value: “Pop3”
Allowed values:

Value	Description
“Pop3”	
“IMAP”	
“Active Sync”	Microsoft Active sync protocol

./Com.SonyEricsson/Settings/Email/EmailAcc/X/Incoming/Security

Used security method.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Default Value: "None"
Allowed values:

Value	Description
"None"	
"SSL"	Secure connection over specified port
"TLS"	Secure MAP over TLS

./Com.SonyEricsson/Settings/Email/EmailAcc/X/Incoming/AuthInfo

Container for authentication information for the incoming server.

Access Type: Add, Get, Replace
Occurrence: One
Format: Node

./Com.SonyEricsson/Settings/Email/EmailAcc/X/Incoming/AuthInfo/AuthName

User name for incoming server.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 128

./Com.SonyEricsson/Settings/Email/EmailAcc/X/Incoming/AuthInfo/AuthSecret

Password for incoming server.

Access Type: Add, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 40

./Com.SonyEricsson/Settings/Email/EmailAcc/X/Outgoing

Settings for outgoing mail.

Access Type: Add, Get
Occurrence: ZeroOrOne
Format: Node

./Com.SonyEricsson/Settings/Email/EmailAcc/X/Outgoing/Addr

Outgoing server address.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 31

./Com.SonyEricsson/Settings/Email/EmailAcc/X/Outgoing/PortNbr

Port number.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default Value: 25
Allowed values: Integer in range 0 to 65535

./Com.SonyEricsson/Settings/Email/EmailAcc/X/Outgoing/Security

Used security method.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Default Value: "None"
Allowed values:

Value	Description
"None"	
"SSL"	Secure connection over specified port
"TLS"	Secure MAP over TLS

./Com.SonyEricsson/Settings/Email/EmailAcc/X/Outgoing/AuthInfo

Container for information server authentication information.

Access Type: Add, Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Settings/Email/EmailAcc/X/Outgoing/AuthInfo/AuthName

SMTP user name.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 128

./Com.SonyEricsson/Settings/Email/EmailAcc/X/Outgoing/AuthInfo/AuthSecret

SMTP user password.

Access Type: Add, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 40

./Com.SonyEricsson/Settings/Email/EmailAcc/X/Outgoing/AuthInfo/AuthState

Authentication state used for the outgoing server.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Default Value: “Disabled”
Allowed values:

Value	Description
“Disabled”	SMTP authentication is disabled
“Enabled”	SMTP authentication is enabled
“Use incoming”	SMTP authentication is enabled and the incoming credentials are used

./Com.SonyEricsson/Settings/Email/EmailAcc/X/AutomaticDownload

Automatic download of new mail.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Default Value: “headers and text and attachments”
Allowed values:
“headers and text"
"headers only"
"headers and text and attachments"

./Com.SonyEricsson/Settings/Email/EmailAcc/X/AutomaticDownloadLimit

Max number of KB downloaded automatically during a folder sync. 0 = unlimited.

Access Type: Add, Get, Replace
Occurrence: One
Format: int
Default Value: 10
Allowed values: Integer in range 0 to 10 000

./Com.SonyEricsson/Settings/Email/EmailAcc/X/AllowRoaming

Selection if automatic connections are allowed from the user home network only, or from any network.

Access Type: Add, Get, Replace
Occurrence: One
Format: bool
Default Value: False

./Com.SonyEricsson/Settings/Email/EmailAcc/X/FolderSize

Set the number of emails to hold in the inbox folder and to fetch during a "check new mail" operation. 0 = unlimited.

Access Type: Add, Get, Replace
Occurrence: One
Format: int
Default Value: 100
Allowed values: Integer in range 0 to 10 000

./Com.SonyEricsson/Settings/Email/EmailAcc/X/CheckMailsInterval

Automatic poll interval (in seconds).

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: int
Default Value: 0
Allowed values:
0
300
1800
3600
7200
10800
14400
43200

./Com.SonyEricsson/Settings/Email/EmailAcc/X/PushEmail

This node enables/disables Push email via inband notifications (IMAP IDLE). Requires server support.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Default Value: "`not-available`"
Allowed values:

Value	Description
"`not-available`"	Not supported by server
"`off`"	Turned off
"`on`"	Turned on

./Com.SonyEricsson/Settings/Email/EmailAcc/X/AutoDelete

True if messages which are no longer present on the server should automatically be removed from the phone as well.

Access Type: Add, Get, Replace
Occurrence: One
Format: bool
Default Value: True

./Com.SonyEricsson/Settings/Email/EmailAcc/X/PrefConRef

This node specifies a reference to preferred data account object for connectivity, for example,
"`./AP/AP-01`".

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Default Value: "`Pop3`"
Allowed values: "`./AP/<X>`", where <X> is the placeholder name for the linked account. This account must exist in the tree.

./Com.SonyEricsson/Settings/Email/EmailAcc/X/AllowLocalBearer

True if incoming connections should use any available local bearers, false to force GPRS/UMTS.

Access Type: Add, Get, Replace
Occurrence: One
Format: bool
Default Value: True

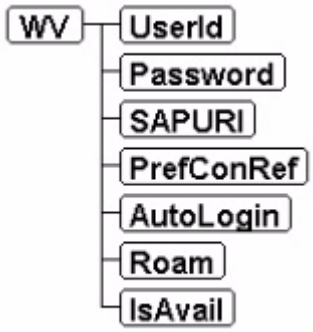
./Com.SonyEricsson/Settings/Email/ActiveAcc

Access Type: Get, Replace
Occurrence: One
Format: chr

My Friends (Wireless Village) settings

Note: This subtree is **not supported** in phones with DM client version 6.

Subtree structure



./Com.SonyEricsson/Settings/WV

Settings for the "My Friends" application (Wireless Village).

Access Type: Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Settings/WV/UserId

User ID.

Access Type: Get, Replace
Occurrence: One
Format: chr
Allowed values: String, max length 50, Format: “`wv:user@domain`”

./Com.SonyEricsson/Settings/WV/Password

User password.

Access Type: Replace
Occurrence: One
Format: chr
Allowed values: String, max length 50

./Com.SonyEricsson/Settings/WV/SAPURI

Server URL.

Access Type: Get, Replace
Occurrence: One
Format: chr
Allowed values: String, max length 200, URL

./Com.SonyEricsson/Settings/WV/ProxyRef

Path to the data account placeholder in the DM tree which holds the data account to be used, for example, "`./AP/AP-01`".

Access Type: Get, Replace
Occurrence: One
Format: chr
Allowed values: "`./AP/<X>`", where <X> is the placeholder name for the linked account. This account must exist in the tree.

./Com.SonyEricsson/Settings/WV/AutoLogin

Indicates if auto-login is enabled.

Access Type: Get, Replace
Occurrence: One
Format: bool
Default Value: False

./Com.SonyEricsson/Settings/WV/Roam

Allows connection if roaming.

Access Type: Get, Replace
Occurrence: One
Format: bool
Default Value: False

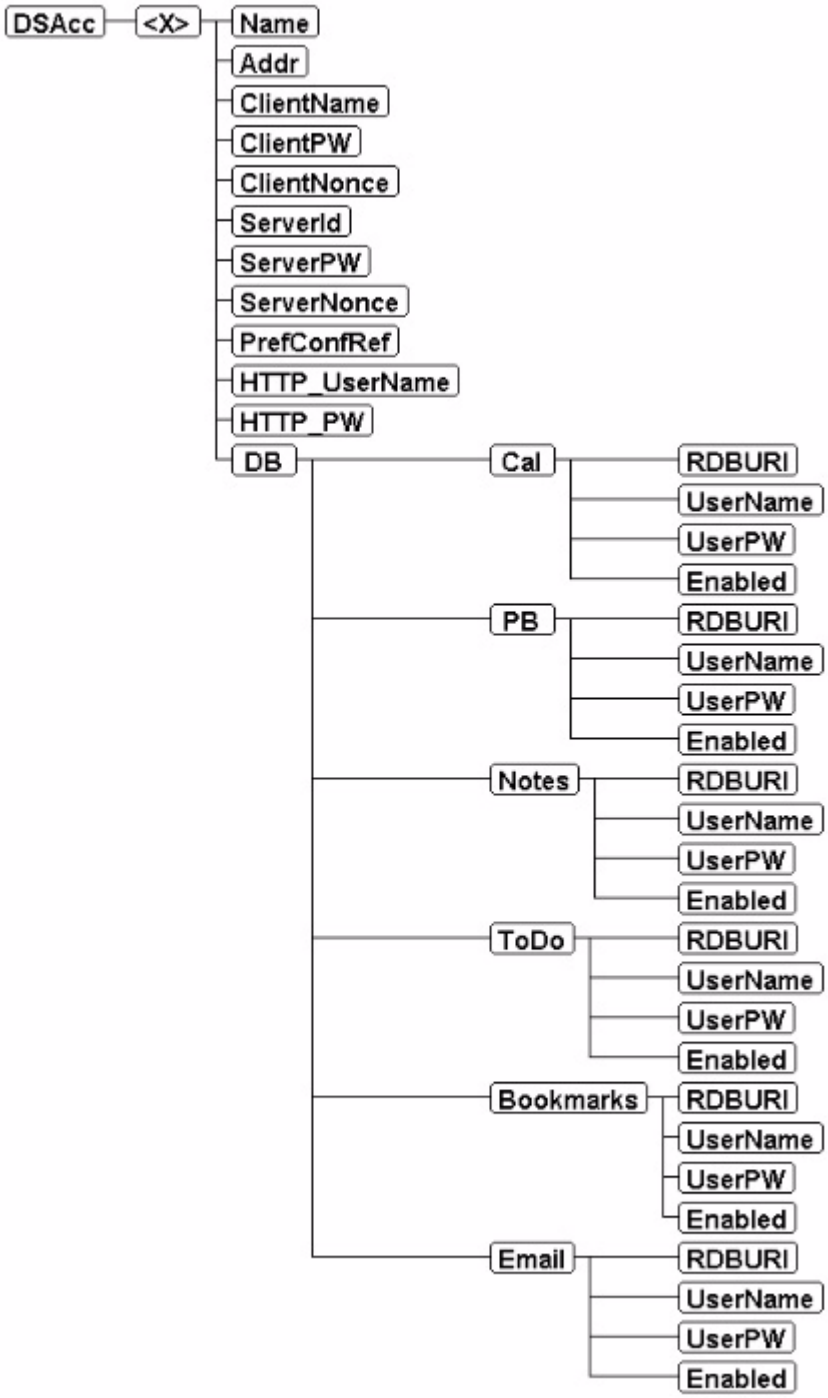
./Com.SonyEricsson/Settings/WV/IsAvail

Indicates if the application is enabled (read-only).

Access Type: Get
Occurrence: One
Format: bool
Default Value: True

OMA Data Sync accounts

Subtree structure



./Com.SonyEricsson/Settings/Sync/DSAcc

OMA DS 1.2 accounts.

Access Type: Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Settings/Sync/DSAcc/X

Access Type: Add, Delete, Get
Occurrence: ZeroOrN (N<=5)
Format: Node

./Com.SonyEricsson/Settings/Sync/DSAcc/X/Name

Displayable name for this account.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 49

./Com.SonyEricsson/Settings/Sync/DSAcc/X/Addr

Server address, the URL to the sync server.

Access Type: Add, Get, Replace
Occurrence: One
Format: chr
Allowed values: String, max length 155, URL

./Com.SonyEricsson/Settings/Sync/DSAcc/X/ClientName

Client identity, used for client authentication.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 79

./Com.SonyEricsson/Settings/Sync/DSAcc/X/ClientPW

Client password, used for client authentication.

Access Type: Add, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 59

./Com.SonyEricsson/Settings/Sync/DSAcc/X/ClientNonce

Next nonce to be used for client authentication.

Access Type: Add, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 34 bytes

./Com.SonyEricsson/Settings/Sync/DSAcc/X/ServerId

Server identity used for server authentication.

Access Type: Add, Get, Replace
Occurrence: One
Format: chr
Allowed values: String, max length 79

./Com.SonyEricsson/Settings/Sync/DSAcc/X/ServerPW

Server password, used for server authentication.

Access Type: Add, Replace
Occurrence: One
Format: chr
Allowed values: String, max length 59

./Com.SonyEricsson/Settings/Sync/DSAcc/X/ServerNonce

Access Type: Add, Replace
Occurrence: One
Format: chr
Allowed values: String, max length 34

./Com.SonyEricsson/Settings/Sync/DSAcc/X/ProxyRef

This node specifies a reference to preferred data account object for connectivity, for example,
"./AP/AP-01"

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: "./AP/<X>", where <X> is the placeholder name for the linked account. This account must exist in the tree.

./Com.SonyEricsson/Settings/Sync/DSAcc/X/HTTP_UserName

Username for HTTP authentication.

Access Type: Add, Get, Replace
Occurrence: One
Format: chr
Allowed values: String, max length 79

./Com.SonyEricsson/Settings/Sync/DSAcc/X/HTTP_PW

Password for HTTP authentication.

Access Type: Add, Replace
Occurrence: One
Format: chr
Allowed values: String, max length 59

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB

Sync databases.

Access Type: Add, Get
Occurrence: ZeroOrOne
Format: Node

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/Cal

Application settings for Calendar sync.

Access Type: Add, Get
Occurrence: ZeroOrOne
Format: Node

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/Cal/RDBURI

Database name.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 99

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/Cal/UserName

Username.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 79

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/Cal/UserPW

Password.

Access Type: Add, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 59

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/Cal/Enabled

Indicates if this application should be synchronised.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: bool
Default Value: False

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/PB

Application settings for Contacts (Phonebook) sync.

Access Type: Add, Get
Occurrence: ZeroOrOne
Format: Node

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/PB/RDBURI

Database name.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 99

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/PB/UserName

User name.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 79

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/PB/UserPW

Password.

Access Type: Add, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 59

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/PB/Enabled

Indicates if this application should be synchronised.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: bool
Default Value: False

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/Notes

Application settings for Notes sync.

Access Type: Add, Get
Occurrence: ZeroOrOne
Format: Node

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/Notes/RDBURI

Database name.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 99

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/Notes/UserName

User name.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 79

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/Notes/UserPW

Password.

Access Type: Add, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 59

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/Notes/Enabled

Indicates if this application should be synchronised.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: bool
Default Value: False

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/ToDo

Application settings for Tasks sync.

Access Type: Add, Get
Occurrence: ZeroOrOne
Format: Node

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/ToDo/RDBURI

Database name.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 99

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/ToDo/UserName

User name.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 79

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/ToDo/UserPW

Password.

Access Type: Add, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 59

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/ToDo/Enabled

Indicates if this application should be synchronised.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: bool
Default Value: False

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/Bookmarks

Application settings for Bookmarks sync.

Access Type: Add, Get
Occurrence: ZeroOrOne
Format: Node

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/Bookmarks/RDBURI

Database name.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 99

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/Bookmarks/UserName

User name.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 79

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/Bookmarks/UserPW

Password.

Access Type: Add, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 59

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/Bookmarks/Enabled

Indicates if this application should be synchronised.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: bool
Default Value: False

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/Email

Application settings for Email sync.

Access Type: Add, Get
Occurrence: ZeroOrOne
Format: Node

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/Email/RDBURI

Database name.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 99

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/Email/UserName

User name.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 79

./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/Email/UserPW

Password.

Access Type: Add, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values: String, max length 59

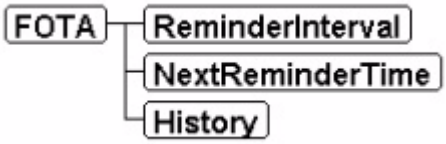
./Com.SonyEricsson/Settings/Sync/DSAcc/X/DB/Email/Enabled

Indicates if this application should be synchronised.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: bool
Default Value: False

Sony Ericsson Update Service

Subtree structure



./Com.SonyEricsson/Settings/FOTA

Settings for the Sony Ericsson Update Service application.

Access Type: Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Settings/FOTA/ReminderInterval

This node specifies when the next notification is presented to the user.

Access Type: Get, Replace
Occurrence: One
Format: chr
Default Value: “Off“
Allowed values:

Value	Description
“Off”	No automatic reminders
“At Startup”	Reminder when the phone starts up
“3 Month”	Reminder every three months

./Com.SonyEricsson/Settings/FOTA/NextReminderTime

(Read only) The UTC DateTime for the next notification if ReminderInterval is set to "1 Month". When ReminderInterval is "Off" or "At Startup", the value is 0.

Access Type: Get
Occurrence: One
Format: int
Default Value: 0
Allowed values: Integer, number of seconds since midnight 1/1 1970 to the time for the next reminder

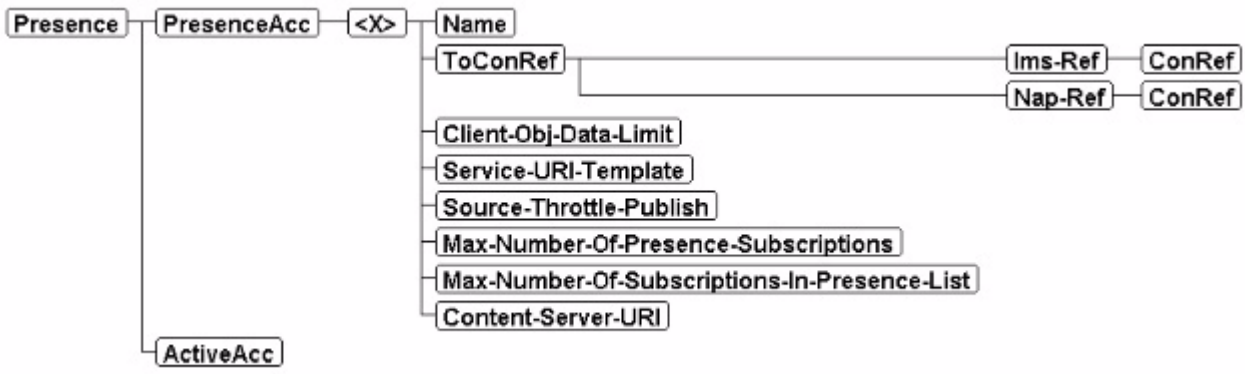
./Com.SonyEricsson/Settings/FOTA/History

(Read-only) History log of Firmware Update operations, in readable ASCII plain text.

Access Type: Get
Occurrence: One
Format: chr

Presence and availability Management Object

Subtree structure



./Com.SonyEricsson/Settings/Presence

OMA standardised Management Object for presence and availability.

Access Type: Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Settings/Presence/PresenceAcc

Access Type: Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Settings/Presence/PresenceAcc/X

Access Type: Add, Delete, Get
Occurrence: ZeroOrN (N<=1)
Format: Node

./Com.SonyEricsson/Settings/Presence/PresenceAcc/X/Name

Displayable application name. It is specific for each service provider.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr

./Com.SonyEricsson/Settings/Presence/PresenceAcc/X/ToConRef

This interior node is used as a container to allow several connectivity references. (Currently only one static object is supported by this implementation.)

Access Type: Add, Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Settings/Presence/PresenceAcc/X/ToConRef/Ims-Ref

A placeholder for a connectivity reference.

Access Type: Add, Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Settings/Presence/PresenceAcc/X/ToConRef/Ims-Ref/ConRef

This node specifies a reference to preferred data account object for connectivity, for example,
"./AP/AP-01"

Access Type: Add, Get, Replace
Occurrence: One
Format: chr
Allowed values: "./AP/<X>", where <X> is the placeholder name for the linked account. This account must exist in the tree.

./Com.SonyEricsson/Settings/Presence/PresenceAcc/X/ToConRef/Nap-Ref

Access Type: Add, Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Settings/Presence/PresenceAcc/X/Nap-Ref/ConRef

This node specifies a reference to preferred data account object for connectivity, for example,
"./AP/AP-01"

Access Type: Add, Get, Replace
Occurrence: One
Format: chr
Allowed values: "./AP/<X>", where <X> is the placeholder name for the linked account. This account must exist in the tree.

./Com.SonyEricsson/Settings/Presence/PresenceAcc/X/Client-Obj-Data-Limit

This parameter defines the maximum size of the MIME object in SIP PUBLISH.

Access Type: Add, Get, Replace
Occurrence: One
Format: int

./Com.SonyEricsson/Settings/Presence/PresenceAcc/X/Service-URI-Template

The Service URI Template specifies the syntax of the service URI. The Service URI Template SHALL be a URI Template as specified in the XDM specification, subclause C.1

Access Type: Add, Get, Replace
Occurrence: One
Format: chr
Allowed values: String, a SIP URI

./Com.SonyEricsson/Settings/Presence/PresenceAcc/X/Source-Throttle-Publish

This node defines the minimum time interval (in seconds) between two consecutive publications from a presence source.

Access Type: Add, Get, Replace
Occurrence: One
Format: int

./Com.SonyEricsson/Settings/Presence/PresenceAcc/X//Max-Number-Of-Presence-Subscriptions

This node limits the number of presence subscriptions.

Access Type: Add, Get, Replace
Occurrence: One
Format: int

./Com.SonyEricsson/Settings/Presence/PresenceAcc/X/Max-Number-Of-Subscriptions-In-Presence-List

This parameter limits the number of back-end subscriptions allowed for a presence list.

Access Type: Add, Get, Replace
Occurrence: One
Format: int

./Com.SonyEricsson/Settings/Presence/PresenceAcc/X/Content-Server-URI

This parameter defines the HTTP URI of the content server to be used for content indirection.

Access Type: Add, Get, Replace
Occurrence: One
Format: chr

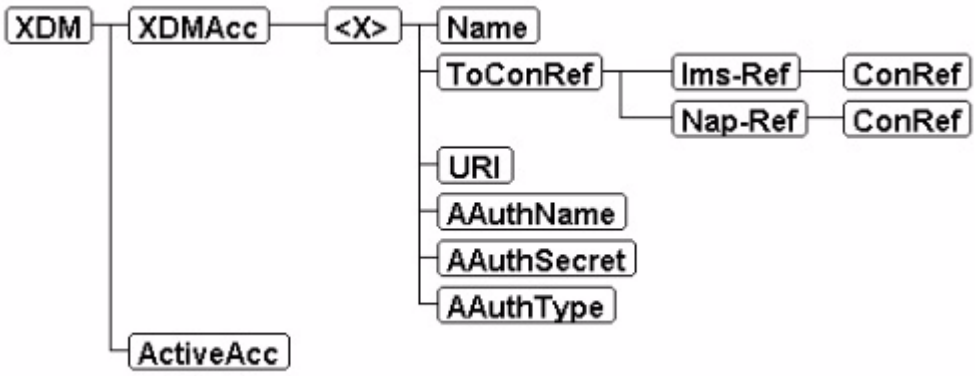
./Com.SonyEricsson/Settings/Presence/ActiveAcc

Name of the currently active presence account placeholder in the DM tree, for example, "PresenceAcc-01" or "./Com.SonyEricsson/Settings/Presence/PresenceAcc/PresenceAcc-01", if an account named "PresenceAcc-01" exists. If the number of accounts is limited to 1, ActiveAcc is configured automatically.

Access Type: Add, Get, Replace
Occurrence: One
Format: chr
Allowed values: "./Com.SonyEricsson/Settings/Presence/PresenceAcc/<X>" or "<X>", where <X> is the placeholder name for the linked account. This account must exist in the tree.

XDM Management Object

Subtree structure



./Com.SonyEricsson/Settings/XDM

OMA standardised Management Object for presence and availability, used for XDM continuous provisioning.

Access Type: Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Settings/XDM/XDMAcc

Access Type: Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Settings/XDM/XDMAcc/X

A static placeholder for one instance of XDM settings.

Access Type: Add, Delete, Get
Occurrence: ZeroOrN (N<=1)
Format: Node

./Com.SonyEricsson/Settings/XDM/XDMAcc/X/Name

Displayable application name. It is specific for each service provider.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr

./Com.SonyEricsson/Settings/XDM/XDMAcc/X/ToConRef

The ToConRef interior node is used to allow several connectivity references. (Currently only one static object is supported by this implementation.)

Access Type: Add, Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Settings/XDM/XDMAcc/X/ToConRef/Ims-Ref

This node specifies a reference to an ims account object, for example, "`./Com.Sonyericsson/settings/ims/imsacc/<X>`" or "`<X>`"

Access Type: Add, Get
Occurrence: One
Format: Node
Allowed values: "`./Com.Sonyericsson/settings/ims/imsacc/<X>`", where <X> is the placeholder name for the linked account. This account must exist in the tree.

./Com.SonyEricsson/Settings/XDM/XDMAcc/X//ToConRef/Ims-Ref/ConRef

The ConRef indicates the linkage to connectivity parameters. The value is a path to the data account placeholder in the DM tree which holds the data account to be used, for example,
"`./AP/AP-01`".

Access Type: Add, Get, Replace
Occurrence: One
Format: chr
Allowed values: "`./AP/X`", where X is the placeholder name for the linked account. This account must exist in the tree.

./Com.SonyEricsson/Settings/XDM/XDMAcc/X/ToConRef/Nap-Ref

This node specifies a reference to preferred AP object for connectivity, for example, "`./AP/AP-01`"

Access Type: Add, Get
Occurrence: One
Format: Node
Allowed values: "`./AP/<X>`" or "`<X>`", where <X> is the placeholder name for the linked account. This account must exist in the tree.

./Com.SonyEricsson/Settings/XDM/XDMAcc/X/ToConRef/Nap-Ref/ConRef

The ConRef indicates the linkage to connectivity parameters. The value is a path to the data account placeholder in the DM tree which holds the data account to be used, for example,
"./AP/AP-01".

Access Type: Add, Get, Replace
Occurrence: One
Format: chr
Allowed values: "./AP/X", where X is the placeholder name for the linked account. This account must exist in the tree.

./Com.SonyEricsson/Settings/XDM/XDMAcc/X/URI

This parameter defines the root of all XDM resources (this is the Aggregation Proxy address). This is useful when accessing via XCAP.

Access Type: Add, Get, Replace
Occurrence: One
Format: chr

./Com.SonyEricsson/Settings/XDM/XDMAcc/X/AAuthName

This parameter defines the user name for XDMC authentication using HTTP digest.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr

./Com.SonyEricsson/Settings/XDM/XDMAcc/X/AAuthSecret

This parameter defines the password for XDMC authentication using HTTP digest.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr

./Com.SonyEricsson/Settings/XDM/XDMAcc/X/AAuthType

This parameter defines the authentication type for XDMC authentication.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr
Allowed values:

Value	Description
“GAA”	The authentication method is GAA
“Digest”	The authentication method is HTTP digest

./Com.SonyEricsson/Settings/XDM/ActiveAcc

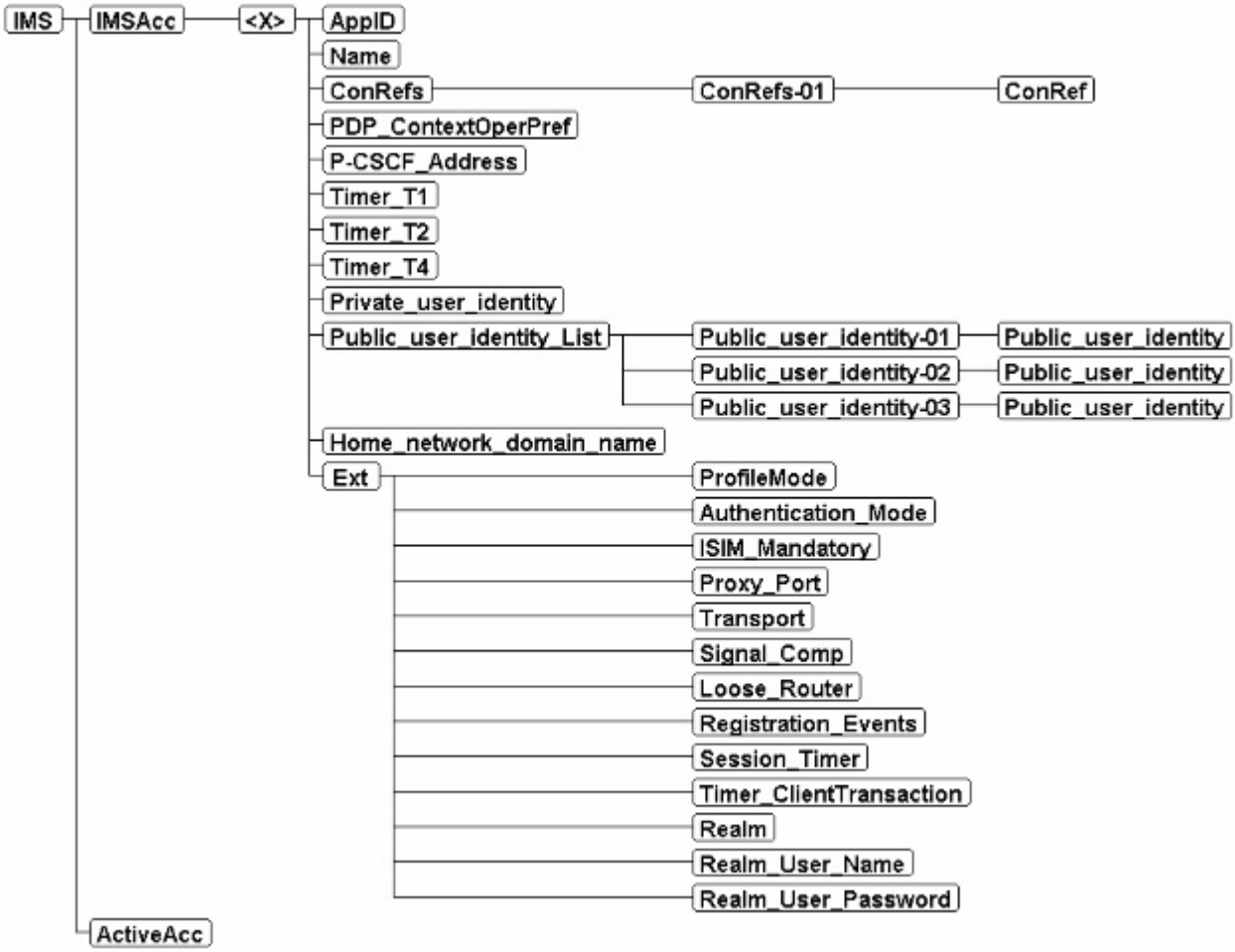
Name of the currently active XDM account placeholder in the DM tree, for example, "`XDMAcc-01`" or "`./Com.SonyEricsson/Settings/XDM/XDMAcc/XDMAcc-01`", if an account named "`XDMAcc-01`" exists. If the number of accounts is limited to 1, ActiveAcc is configured automatically.

Access Type: Get, Replace
Occurrence: One
Format: chr
Allowed values: "`./Com.Sonyericsson/settings/XDM/XDMAcc/<X>`", where <X> is the placeholder name for the linked account. This account must exist in the tree.

IP Multimedia Subsystem (IMS) Management Object

Note: IMS is **not** supported in phones with DM version 6.

Subtree structure



./Com.SonyEricsson/Settings/IMS

3GPP standardised Management Object for IP Multimedia Subsystem (IMS).

Access Type: Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Settings/IMS/IMSAcc

Access Type: Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Settings/IMS/IMSAcc/X

A static placeholder for one instance of IMS settings. (Please refer to the 3GPP standard documentation for details on the settings.)

Access Type: Add, Delete, Get, Replace
Occurrence: ZeroOrN (N<=1)
Format: Node

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/AppID

This node specifies the application ID for IMS account object.

Access Type:Get
Occurrence: One
Format: chr
Default value: “`ap2001`”

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/Name

Displayable application name. It is specific for each service provider.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/ConRefs

This interior node is used as a container to allow several connectivity references. (Currently only one static object is supported by this implementation.)

Access Type: Add, Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/ConRefs/ConRefs-01

A placeholder for a connectivity reference.

Access Type: Add, Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/ConRefs/ConRefs-01/ConRef

This node specifies a reference to preferred data account object for connectivity, for example,
"`./AP/AP-01`"

Access Type: Add, Get, Replace
Occurrence: One
Format: chr
Allowed values: "`./AP/<X>`", where <X> is the placeholder name for the linked account. This account must exist in the tree.

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/PDP_ContextOperPref

The PDP_ContextOperPref leaf indicates an operator's preference to have a dedicated PDP context for SIP signalling.

Access Type: Add, Get, Replace
Occurrence: One
Format: bool
Default value: False

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/P-CSCF_Address

The P-CSCF_Address leaf defines an FQDN to an IPv4 P-CSCF.

Access Type: Add, Get, Replace
Occurrence: ZeroOrOne
Format: chr

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/Timer_T1

SIP timer T1 – round trip time given in milliseconds.

Access Type: Add, Get, Replace
Occurrence: One
Format: int

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/Timer_T2

SIP timer T2 – the maximum retransmit interval for non-INVITE requests and INVITE responses, in milliseconds.

Access Type: Add, Get, Replace
Occurrence: One
Format: int

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/Timer_T4

SIP timer T4 – the maximum duration a message will remain in the network, in milliseconds.

Access Type: Add, Get, Replace
Occurrence: One
Format: int

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/Private_user_identity

Represents the private user identity.

Access Type: Add, Get, Replace
Occurrence: One
Format: chr

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/Public_user_identity_List

This interior node is a container for multiple Public User Identity elements.

Access Type: Add, Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/Public_user_identity_List/Public_user_identity-01

The current client implementation only supports a fixed number of elements.

Access Type: Add, Get
Occurrence: ZeroOrN (N<=3)
Format: Node

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/Public_user_identity_List/Public_user_identity-01/Public_user_identity

Public user identity.

Access Type: Add, Get, Replace
Occurrence: ZeroOrN (N<=3)
Format: chr

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/Public_user_identity_List/Public_user_identity-02

Access Type: Add, Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/Public_user_identity_List/Public_user_identity-02/Public_user_identity

Access Type: Add, Get, Replace
Occurrence: One
Format: chr

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/Public_user_identity_List/Public_user_identity-03

Access Type: Add, Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/Public_user_identity_List/Public_user_identity-03/Public_user_identity

Access Type: Add, Get, Replace
Occurrence: One
Format: chr

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/Home_network_domain_name

Indicates the operator home network domain.

Access Type: Add, Get, Replace
Occurrence: One
Format: chr

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/Ext

Interior node containing Sony Ericsson specific extensions to the standardised MO.

Access Type: Add, Get
Occurrence: ZeroOrOne
Format: Node

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/Ext/ProfileMode

Profile mode.

Access Type: Add, Get, Replace
Occurrence: One
Format: int
Default value: 1
Allowed values:

Value	Description
0	EITF
1	IMS

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/Ext/Authentication_Mode

This setting specifies the type of authentication to use in IMS mode.

Access Type: Add, Get, Replace
Occurrence: One
Format: int
Default value: 1
Allowed values:

Value	Description
0	EARLY_IMS
1	FULL_IMS
2	FALLBACK. Fallback mode tries full IMS security first, and, only if it fails, reverts to early IMS security

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/Ext/ISIM_Mandatory

Flag to enforce presence of ISIM.

Access Type: Add, Get, Replace
Occurrence: One
Format: bool
Default value: False

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/Ext/Proxy_Port

Proxy port used in Early IMS implementations.

Access Type: Add, Get, Replace
Occurrence: One
Format: int
Default value: 5060
Allowed values: Integer in range 0 to 65535

./Com.SonyEricsson/Sett fsings/IMS/IMSAcc/X/Ext/Transport

Transport protocol used between UE and proxy.

Access Type: Add, Get, Replace
Occurrence: One
Format: int
Default value: 0
Allowed values:

Value	Description
0	UDP
1	TCP

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/Ext/Signal_Comp

Use signal compression.

Access Type: Add, Get, Replace
Occurrence: One
Format: bool
Default value: False

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/Ext/Loose_Router

Flag to enable loose routing.

Access Type: Add, Get, Replace
Occurrence: One
Format: bool
Default value: True

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/Ext/Registration_Events

Flag to enable subscription to registration events after successful registration. Used for network initiated deregistration or reauthentication.

Access Type: Add, Get, Replace
Occurrence: One
Format: bool
Default value: True

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/Ext/Session_Timer

Non-zero value indicates session expiry timer value, 0 disables timer.

Access Type: Add, Get, Replace
Occurrence: One
Format: int
Default value: 1800

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/Ext/Timer_ClientTransaction

Maximum lifetime for a SIP client transaction. Given in milliseconds.

Access Type: Add, Get, Replace
Occurrence: One
Format: int
Default value: 180 000

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/Ext/Realm

IETF mode only. Specifies the realm to use for authentication.

Access Type: Add, Get, Replace
Occurrence: One
Format: chr

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/Ext/Realm_User_Name

IETF mode only. Specifies the user name to use for authentication.

Access Type: Add, Get, Replace
Occurrence: One
Format: chr

./Com.SonyEricsson/Settings/IMS/IMSAcc/X/X/Ext/Realm_User_Password

IETF mode only. Specifies the user password to use for authentication.

Access Type: Add, Replace
Occurrence: One
Format: chr

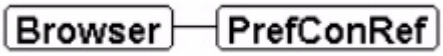
./Com.SonyEricsson/Settings/IMS/ActiveAcc

Name of the currently active IMS account placeholder in the DM tree, for example, "IMSAcc-01" or "./Com.SonyEricsson/Settings/IMS/IMSAcc/IMSAcc-01", if an account named "IMSAcc-01" exists.

Access Type: Get, Replace
Occurrence: One
Format: chr
Allowed values: "./Com.SonyEricsson/Settings/IMS/IMSAcc/<X>", where <X> is the placeholder name for the linked account. This account must exist in the tree.

Browser settings

Subtree structure



./Com.SonyEricsson/Settings/Browser

Settings for the Browser application.

Access Type: Get
Occurrence: One
Format: Node

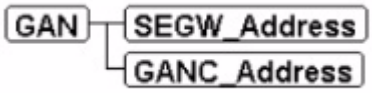
./Com.SonyEricsson/Settings/Browser/PrefConRef

This node specifies a reference to the preferred data account object for connectivity, for example,
"./AP/AP-01"

Access Type: Get, Replace
Occurrence: One
Format: chr
Allowed values: "./AP/<X>", where <X> is the placeholder name for the linked account. This account must exist in the tree.

Generic Access Network (GAN) settings

Subtree structure



./Com.SonyEricsson/Settings/GAN

Settings for Generic Access Network application..

Access Type: Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Settings/GAN/SEGW_Address

The Fully Qualified Domain Name (FQDN) address of the security gateway.

Access Type: Get, Replace
Occurrence: ZeroOrOne
Format: chr

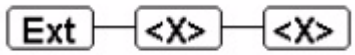
./Com.SonyEricsson/Settings/GAN/GANC_Address

The Fully Qualified Domain Name (FQDN) address of the gan server.

Access Type: Get, Replace
Occurrence: ZeroOrOne
Format: chr

Dummy tree extensions

Subtree structure



./Com.SonyEricsson/Ext

The Ext subtree is an area where undefined dummy nodes can be added. Primarily for testing purposes, these nodes will be added to the DM tree but not affect the device or its applications in any way (other than consuming space).

Access Type: Get
Occurrence: One
Format: Node

./Com.SonyEricsson/Ext/X

Dummy nodes must be placed within a placeholder.

Access Type: Add, Delete, Get, Replace
Occurrence: ZeroOrMore
Format: Node

./Com.SonyEricsson/Ext/X/X

Dummy nodes can have any name and any format except Node. That is, it is only possible to have one level of interior placeholders under Ext.

Access Type: Add, Delete, Get, Replace
Occurrence: ZeroOrMore
Format: null

General DM examples

The following examples are valid for DM clients with DevInfo/DmV = 5.x.

Adding a new DM account

Note: Example data, like server addresses, are for illustrative purposes only.

```
<SyncBody>
   <Add>
      <CmdID>4</CmdID>
      <Item>
         <Target>
            <LocURI>./DMAcc/aDMAccountName</LocURI>
         </Target>
         <Meta>
            <Format xmlns="syncml:metinf">node</Format>
         </Meta>
      </Item>
   </Add>
   <Add>
      <CmdID>5</CmdID>
      <Item>
         <Target>
            <LocURI>./DMAcc/aDMAccountName/ServerID</LocURI>
         </Target>
         <Data>aServerID</Data>
      </Item>
      <Item>
         <Target>
            <LocURI>./DMAcc/aDMAccountName/Name</LocURI>
         </Target>
         <Data>DisplayableAccountName</Data>
      </Item>
      <Item>
         <Target>
            <LocURI>./DMAcc/aDMAccountName/PrefConRef</LocURI>
         </Target>
         <Data>./AP/AP-01</Data>
      </Item>
      <Item>
         <Target>
            <LocURI>./DMAcc/aDMAccountName/AppAddr</LocURI>
         </Target>
         <Meta>
            <Format xmlns="syncml:metinf">node</Format>
         </Meta>
      </Item>
      <Item>
         <Target>
            <LocURI>./DMAcc/aDMAccountName/AppAddr/
anAppAddrPlaceholderName</LocURI>
```

```
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
      <Item>
        <Target>
          <LocURI>./DMAcc/aDMAccountName/AppAddr/
anAppAddrPlaceholderName/Addr</LocURI>
        </Target>
        <Data>https://some.server.com</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./DMAcc/aDMAccountName/AppAddr/
anAppAddrPlaceholderName/AddrType</LocURI>
        </Target>
        <Data>URI</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./DMAcc/aDMAccountName/AppAddr/
anAppAddrPlaceholderName/Port</LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
      <Item>
        <Target>
          <LocURI>./DMAcc/aDMAccountName/AppAddr/
anAppAddrPlaceholderName/Port/anPortPlaceholderName</LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
      <Item>
        <Target>
          <LocURI>./DMAcc/aDMAccountName/AppAddr/
anAppAddrPlaceholderName/Port/anPortPlaceholderName/PortNbr</
LocURI>
        </Target>
        <Data>65535</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./DMAcc/aDMAccountName/AAuthPref</LocURI>
        </Target>
        <Data>BASIC</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./DMAcc/aDMAccountName/AppAuth</LocURI>
        </Target>
```

```
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
      <Item>
        <Target>
          <LocURI>./DMAcc/aDMAccountName/AppAuth/
anAppAuthPlaceholderName</LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
      <Item>
        <Target>
          <LocURI>./DMAcc/aDMAccountName/AppAuth/
anAppAuthPlaceholderName/AAuthLevel</LocURI>
        </Target>
        <Data>SRVCRED</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./DMAcc/aDMAccountName/AppAuth/
anAppAuthPlaceholderName/AAuthName</LocURI>
        </Target>
        <Data>AAuthName</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./DMAcc/aDMAccountName/AppAuth/
anAppAuthPlaceholderName/AAuthSecret</LocURI>
        </Target>
        <Data>AAuthSecret</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./DMAcc/aDMAccountName/AppAuth/
firstAppAuthPlaceholderName/AAuthData</LocURI>
        </Target>
        <Data>NextNonce</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./DMAcc/aDMAccountName/Ext</LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
      <Item>
        <Target>
          <LocURI>./DMAcc/aDMAccountName/Ext/Locked</LocURI>
        </Target>
        <Data>false</Data>
      </Item>
```

```
      <Item>
        <Target>
          <LocURI>./DMAcc/aDMAccountName/Ext/
UserEditable</LocURI>
        </Target>
        <Data>true</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./DMAcc/aDMAccountName/Ext/
AllowClientInitiated</LocURI>
        </Target>
        <Data>true</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./DMAcc/aDMAccountName/Ext/
Notification</LocURI>
        </Target>
        <Data>ask</Data>
      </Item>
   </Add>
</SyncBody>
```

Adding a new NAP (Network Access Point) 3GPPPS

Note: Example data, like server addresses, are for illustrative purposes only.

```
<SyncBody>
   <Add>
      <CmdID>4</CmdID>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId</LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
   </Add>
   <Add>
      <CmdID>5</CmdID>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
Addr</LocURI>
        </Target>
        <Data>Addr</Data>
      </Item>
      <Item>
        <Target>
```

```
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/AuthInfo/
AuthType</LocURI>
        </Target>
        <Data>None</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/AuthInfo/
AuthName</LocURI>
        </Target>
        <Data>AuthName</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/AuthInfo/
AuthSecret</LocURI>
        </Target>
        <Data>AuthSecret</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/IPv4/
AutoConfig</LocURI>
        </Target>
        <Data>True</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/IPv4/
LocalAddr</LocURI>
        </Target>
        <Data>0.0.0.0</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/IPv4/DNS/
DNS-01/DNSAddr</LocURI>
        </Target>
        <Data>0.0.0.0</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/IPv4/
NetMask</LocURI>
        </Target>
        <Data>0.0.0.0</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerType</LocURI>
        </Target>
        <Data>3GPPPS</Data>
      </Item>
      <Item>
```

```
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/</LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS</LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/ReqQos</LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/ReqQos/TrafficClass</LocURI>
        </Target>
        <Data>0</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/ReqQos/DeliveryOrder</LocURI>
        </Target>
        <Data>0</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/ReqQos/DeliveryOfErroneousSDU</LocURI>
        </Target>
        <Data>0</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/ReqQos/MaxSDUsize</LocURI>
        </Target>
        <Data>0</Data>
      </Item>
      <Item>
```

```
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/ReqQos/MaxBitRateForUL</LocURI>
        </Target>
        <Data>0</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/ReqQos/MaxBitRateForDL</LocURI>
        </Target>
        <Data>0</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/ReqQos/ResidualBER</LocURI>
        </Target>
        <Data>7</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/ReqQos/SDUerrorRatio</LocURI>
        </Target>
        <Data>4</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/ReqQos/TransferDelay</LocURI>
        </Target>
        <Data>0</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/ReqQos/TrafficHandlingPriority</LocURI>
        </Target>
        <Data>0</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/ReqQos/GuaranteedBitRateForUL</LocURI>
        </Target>
        <Data>0</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/ReqQos/GuaranteedBitRateForDL</LocURI>
        </Target>
        <Data>0</Data>
      </Item>
```

```
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/ReqQos/SignallingIndication</LocURI>
        </Target>
        <Data>0</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/ReqQos/SourceStatisticsDescriptor</LocURI>
        </Target>
        <Data>0</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/MinQoS</LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/MinQoS/TrafficClass</LocURI>
        </Target>
        <Data>4</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/MinQoS/DeliveryOrder</LocURI>
        </Target>
        <Data>2</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/MinQoS/DeliveryOfErroneousSDU</LocURI>
        </Target>
        <Data>3</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/MinQoS/MaxSDUsize</LocURI>
        </Target>
        <Data>0</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/MinQoS/MaxBitRateForUL</LocURI>
```

```
        </Target>
        <Data>0</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/MinQoS/MaxBitRateForDL</LocURI>
        </Target>
        <Data>0</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/MinQoS/ResidualBER</LocURI>
        </Target>
        <Data>0</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/MinQoS/SDUerrorRatio</LocURI>
        </Target>
        <Data>0</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/MinQoS/TransferDelay</LocURI>
        </Target>
        <Data>0</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/MinQoS/TrafficHandlingPriority</LocURI>
        </Target>
        <Data>0</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/MinQoS/GuaranteedBitRateForUL</LocURI>
        </Target>
        <Data>0</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/MinQoS/GuaranteedBitRateForDL</LocURI>
        </Target>
        <Data>0</Data>
      </Item>
      <Item>
        <Target>
```

```
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/MinQoS/SignallingIndication</LocURI>
        </Target>
        <Data>0</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/MinQoS/SourceStatisticsDescriptor</LocURI>
        </Target>
        <Data>0</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/3GPPPS/Ext</LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
   </Add>
</SyncBody>
```

Adding a new NAP (Network Access Point) WLAN

Note: Example data, like server addresses, are for illustrative purposes only.

```
<SyncML>
   <SyncBody>
      <Add>
        <CmdID>4</CmdID>
        <Item>
          <Target>
            <LocURI>./AP/anAccountName/NAP/aNapObjectId</LocURI>
          </Target>
          <Meta>
            <Format xmlns="syncml:metinf">node</Format>
          </Meta>
        </Item>
      </Add>
      <Add>
        <CmdID>5</CmdID>
        <Item>
          <Target>
            <LocURI>./AP/anAccountName/NAP/aNapObjectId/Addr</
LocURI>
          </Target>
          <Data>Addr</Data>
        </Item>
```

```
        <Item>
          <Target>
            <LocURI>./AP/anAccountName/NAP/aNapObjectId/
AuthInfo/AuthType</LocURI>
          </Target>
          <Data>None</Data>
        </Item>
        <Item>
          <Target>
            <LocURI>./AP/anAccountName/NAP/aNapObjectId/
AuthInfo/AuthName</LocURI>
          </Target>
          <Data>AuthName</Data>
        </Item>
        <Item>
          <Target>
            <LocURI>./AP/anAccountName/NAP/aNapObjectId/
AuthInfo/AuthSecret</LocURI>
          </Target>
          <Data>AuthSecret</Data>
        </Item>
        <Item>
          <Target>
            <LocURI>./AP/anAccountName/NAP/aNapObjectId/IPv4/
AutoConfig</LocURI>
          </Target>
          <Data>True</Data>
        </Item>
        <Item>
          <Target>
            <LocURI>./AP/anAccountName/NAP/aNapObjectId/IPv4/
LocalAddr</LocURI>
          </Target>
          <Data>0.0.0.0</Data>
        </Item>
        <Item>
          <Target>
            <LocURI>./AP/anAccountName/NAP/aNapObjectId/IPv4/
DNS/DNS-01/DNSAddr</LocURI>
          </Target>
          <Data>0.0.0.0</Data>
        </Item>
        <Item>
          <Target>
            <LocURI>./AP/anAccountName/NAP/aNapObjectId/IPv4/
NetMask</LocURI>
          </Target>
          <Data>0.0.0.0</Data>
        </Item>
        <Item>
          <Target>
            <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerType</LocURI>
          </Target>
          <Data>WLAN</Data>
```

```
        </Item>
        <Item>
          <Target>
            <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/</LocURI>
          </Target>
          <Meta>
            <Format xmlns="syncml:metinf">node</Format>
          </Meta>
        </Item>
        <Item>
          <Target>
            <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/WLAN</LocURI>
          </Target>
          <Meta>
            <Format xmlns="syncml:metinf">node</Format>
          </Meta>
        </Item>
        <Item>
          <Target>
            <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/WLAN/SSID</LocURI>
          </Target>
          <Data>SSID</Data>
        </Item>
        <Item>
          <Target>
            <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/WLAN/NetMode</LocURI>
          </Target>
          <Data>INFRA</Data>
        </Item>
        <Item>
          <Target>
            <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/WLAN/SecMode</LocURI>
          </Target>
          <Data>WPA-PSK</Data>
        </Item>
        <Item>
          <Target>
            <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/WLAN/Cipher</LocURI>
          </Target>
          <Data>TKIP</Data>
        </Item>
        <Item>
          <Target>
            <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/WLAN/WPA-PSK</LocURI>
          </Target>
          <Meta>
            <Format xmlns="syncml:metinf">node</Format>
          </Meta>
```

```
        </Item>
        <Item>
          <Target>
            <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/WLAN/WPA-PSK/Data</LocURI>
          </Target>
          <Data>12345678</Data>
        </Item>
        <Item>
          <Target>
            <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/WLAN/WepKeyInd</LocURI>
          </Target>
          <Data>0</Data>
        </Item>
        <Item>
          <Target>
            <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/WLAN/WepAuthMode</LocURI>
          </Target>
          <Data>OPEN</Data>
        </Item>
        <Item>
          <Target>
            <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/WLAN/WepKey</LocURI>
          </Target>
          <Meta>
            <Format xmlns="syncml:metinf">node</Format>
          </Meta>
        </Item>
        <Item>
          <Target>
            <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/WLAN/WepKey/WepKey-01</LocURI>
          </Target>
          <Meta>
            <Format xmlns="syncml:metinf">node</Format>
          </Meta>
        </Item>
        <Item>
          <Target>
            <LocURI>./AP/anAccountName/NAP/aNapObjectId/
BearerParams/WLAN/WepKey/WepKey-01/Data</LocURI>
          </Target>
          <Data>ABCDE</Data>
        </Item>
      </Add>
    <Final/>
    </SyncBody>
</SyncML>
```

Adding proxy settings to an existing AP (Access Point)

Note: Example data, like server addresses, are for illustrative purposes only.

Note: The proxy objects must be connected to a NAP object within the same AP subtree.

```
<SyncBody>
   <Add>
      <CmdID>4</CmdID>
      <Item>
         <Target>
            <LocURI>./AP/anAccountName/Proxy/aProxyObjectId</
LocURI>
         </Target>
         <Meta>
            <Format xmlns="syncml:metinf">node</Format>
         </Meta>
      </Item>
      </Add>
      <Add>
      <CmdID>5</CmdID>
      <Item>
         <Target>
            <LocURI>./AP/anAccountName/Proxy/aProxyObjectId/Addr</
LocURI>
         </Target>
         <Data>proxy.myOperator.com</Data>
      </Item>
      <Item>
         <Target>
            <LocURI>./AP/anAccountName/Proxy/aProxyObjectId/
Ports</LocURI>
         </Target>
         <Meta>
            <Format xmlns="syncml:metinf">node</Format>
         </Meta>
      </Item>
      <Item>
         <Target>
            <LocURI>./AP/anAccountName/Proxy/aProxyObjectId/Ports/
Port-01</LocURI>
         </Target>
         <Meta>
            <Format xmlns="syncml:metinf">node</Format>
         </Meta>
      </Item>
      <Item>
         <Target>
            <LocURI>./AP/anAccountName/Proxy/aProxyObjectId/Ports/
Port-01/PortNbr</LocURI>
         </Target>
         <Data>8080</Data>
```

```
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/Proxy/aProxyObjectId/Ports/
Port-01/Services</LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/Proxy/aProxyObjectId/Ports/
Port-01/Services/Service-01</LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/Proxy/aProxyObjectId/Ports/
Port-01/Services/Service-01/ServiceName</LocURI>
        </Target>
        <Data>http</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/Proxy/aProxyObjectId/Ext</
LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/Proxy/aProxyObjectId/Ext/
Com.SonyEricsson</LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/Proxy/aProxyObjectId/Ext/
Com.SonyEricsson/AuthInfo</LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
      <Item>
        <Target>
```

```
          <LocURI>./AP/anAccountName/Proxy/aProxyObjectId/Ext/
Com.SonyEricsson/AuthInfo/AuthName</LocURI>
        </Target>
        <Data>AuthName</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./AP/anAccountName/Proxy/aProxyObjectId/Ext/
Com.SonyEricsson/AuthInfo/AuthSecret</LocURI>
        </Target>
        <Data>AuthSecret</Data>
      </Item>
   </Add>
</SyncBody>
```

Adding a new MMS profile

Note: Example data, like server addresses, are for illustrative purposes only.

```
<SyncBody>
   <Add>
      <CmdID>4</CmdID>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/MMS/MMSAcc/
anMMSProfile</LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
   </Add>
   <Add>
      <CmdID>5</CmdID>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/MMS/MMSAcc/
anMMSProfile/Name</LocURI>
        </Target>
        <Data>DisplayableName</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/MMS/MMSAcc/
anMMSProfile/MMSC</LocURI>
        </Target>
        <Data>MessageServerAdress</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/MMS/MMSAcc/
anMMSProfile/PrefConRef</LocURI>
        </Target>
```

```
        <Data>./AP/AP-01</Data>
      </Item>
   </Add>
</SyncBody>
```

Adding a new email account

Note: Example data, like server addresses, are for illustrative purposes only.

```
<SyncBody>
   <Add>
      <CmdID>4</CmdID>
      <Item>
         <Target>
            <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName</LocURI>
         </Target>
         <Meta>
            <Format xmlns="syncml:metinf">node</Format>
         </Meta>
      </Item>
      </Add>
      <Add>
      <CmdID>5</CmdID>
      <Item>
         <Target>
            <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/Name</LocURI>
         </Target>
         <Data>DisplayableName</Data>
      </Item>
      <Item>
         <Target>
            <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/FromName</LocURI>
         </Target>
         <Data>FromName</Data>
      </Item>
      <Item>
         <Target>
            <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/FromAddr</LocURI>
         </Target>
         <Data>EmailAdress</Data>
      </Item>
      <Item>
         <Target>
            <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/ReplyToAddr</LocURI>
         </Target>
         <Data>ReplyAdress</Data>
      </Item>
      <Item>
```

```
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/Signature</LocURI>
        </Target>
          <Data>Signature</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/Incoming</LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/Incoming/Addr</LocURI>
        </Target>
        <Data>pop.myOperator.com</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/Incoming/PortNbr</LocURI>
        </Target>
        <Data>110</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/Incoming/ServerProtocol</LocURI>
        </Target>
        <Data>Pop3</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/Incoming/Security</LocURI>
        </Target>
        <Data>None</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/Incoming/AuthInfo</LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
      <Item>
        <Target>
```

```
          <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/Incoming/AuthInfo/AuthName</LocURI>
        </Target>
        <Data>AuthName</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/Incoming/AuthInfo/AuthSecret</LocURI>
        </Target>
        <Data>AuthSecret</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/Outgoing</LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/Outgoing/Addr</LocURI>
        </Target>
          <Data>mail.myOperator.com</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/Outgoing/PortNbr</LocURI>
        </Target>
        <Data>25</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/Outgoing/Security</LocURI>
        </Target>
        <Data>None</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/Outgoing/AuthInfo</LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/Outgoing/AuthInfo/AuthName</LocURI>
```

```
        </Target>
          <Data>Authname</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/Outgoing/AuthInfo/AuthSecret</LocURI>
        </Target>
        <Data>Authsecret</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/Outgoing/AuthInfo/AuthState</LocURI>
        </Target>
        <Data>Disabled</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/AutomaticDownload</LocURI>
        </Target>
        <Data>headers and text and attachments</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/AutomaticDownloadLimit</LocURI>
        </Target>
        <Data>10</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/AllowRoaming</LocURI>
        </Target>
        <Data>false</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/FolderSize</LocURI>
        </Target>
        <Data>100</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/CheckMailsInterval</LocURI>
        </Target>
        <Data>0</Data>
      </Item>
      <Item>
        <Target>
```

```
          <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/PushEmail</LocURI>
        </Target>
        <Data>not-available</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/AutoDelete</LocURI>
        </Target>
        <Data>true</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/PrefConRef</LocURI>
        </Target>
        <Data>./AP/AP-01</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/Email/EmailAcc/
EmailAccountName/AllowLocalBearer</LocURI>
        </Target>
        <Data>true</Data>
      </Item>
   </Add>
</SyncBody>
```

Adding a new IMS account

Note: IMS is **not** supported in phones with DM version 6.

Note: Example data, like server addresses, are for illustrative purposes only.

```
<SyncBody>
   <Add>
      <CmdID>4</CmdID>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount</LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
   </Add>
   <Add>
      <CmdID>5</CmdID>
      <Item>
        <Target>
```

```
          <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Name</LocURI>
        </Target>
        <Data>DisplayableName</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/ConRefs</LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/ConRefs/ConRefs-01</LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/ConRefs/ConRefs-01/ConRef</LocURI>
        </Target>
        <Data>./AP/AP-01</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/PDP_ContextOperPref</LocURI>
        </Target>
        <Data>false</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/P-CSCF_Address</LocURI>
        </Target>
        <Data>P-CSCF_Address</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Timer_T1</LocURI>
        </Target>
        <Data>1</Data>
        </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Timer_T2</LocURI>
```

```
        </Target>
        <Data>1</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Timer_T4</LocURI>
        </Target>
        <Data>1</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Private_user_identity</LocURI>
        </Target>
        <Data>Private_user_identity</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Public_user_identity_List</LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Public_user_identity_List/Public_user_identity-01</
LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Public_user_identity_List/Public_user_identity-01/
Public_user_identity</LocURI>
        </Target>
        <Data>aPublicUserIdentity</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Public_user_identity_List/Public_user_identity-02</
LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
      <Item>
```

```
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Public_user_identity_List/Public_user_identity-02/
Public_user_identity</LocURI>
        </Target>
        <Data>aPublicUserIdentity</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Public_user_identity_List/Public_user_identity-03</
LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Public_user_identity_List/Public_user_identity-03/
Public_user_identity</LocURI>
        </Target>
        <Data>aPublicUserIdentity</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Home_network_domain_name</LocURI>
        </Target>
        <Data>Home_network_domain_name</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Ext</LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">node</Format>
        </Meta>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Ext/Signal_Comp</LocURI>
        </Target>
        <Data>false</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Ext/ProfileMode</LocURI>
        </Target>
        <Data>1</Data>
      </Item>
```

```
     <Item>
       <Target>
         <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Ext/Session_Timer</LocURI>
       </Target>
       <Data>1800</Data>
     </Item>
     <Item>
       <Target>
         <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Ext/Proxy_Port</LocURI>
       </Target>
       <Data>5060</Data>
     </Item>
     <Item>
       <Target>
         <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Ext/Authentication_Mode</LocURI>
       </Target>
       <Data>1</Data>
     </Item>
     <Item>
       <Target>
         <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Ext/ISIM_Mandatory</LocURI>
       </Target>
       <Data>false</Data>
     </Item>
     <Item>
       <Target>
         <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Ext/Transport</LocURI>
       </Target>
       <Data>0</Data>
     </Item>
     <Item>
       <Target>
         <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Ext/Loose_Router</LocURI>
       </Target>
       <Data>true</Data>
     </Item>
     <Item>
       <Target>
         <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Ext/Registration_Events</LocURI>
       </Target>
       <Data>true</Data>
     </Item>
     <Item>
       <Target>
         <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Ext/Timer_ClientTransaction</LocURI>
       </Target>
       <Data>180000</Data>
```

```
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Ext/Realm</LocURI>
        </Target>
        <Data>aRealm</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Ext/Realm_User_Name</LocURI>
        </Target>
        <Data>aRealmUserName</Data>
      </Item>
      <Item>
        <Target>
          <LocURI>./Com.SonyEricsson/Settings/IMS/IMSAcc/
anIMSAccount/Ext/Realm_User_Password</LocURI>
        </Target>
        <Data>aRealmUserPassword</Data>
      </Item>
   </Add>
</SyncBody>
```